



JURIDISKA FAKULTETEN
vid Lunds universitet

Jimmy Serrano

Integritet och kommunikation
– datalagringsdirektivet, Ipred och Telekompaketet
ur ett integritetsperspektiv

Examensarbete
30 högskolepoäng

Handledare
Helén Örnemark Hansen

Ämnesområde
Allmän rättslära, EG-rätt, Immaterialrätt, IT-rätt

Termin
HT-09

Innehåll

SUMMARY	1
SAMMANFATTNING	2
FÖRKORTNINGAR	4
1 INLEDNING	5
2 INTEGRITET	10
2.1 Tidig historik	11
2.2 Privacy – ett nytt integritetsbegrepp	11
2.3 Samtida integritetsbegrepp	13
2.4 Frihet och andra rättigheter	14
2.5 Mänsklig värdighet och intimitet	16
2.6 Rätt till kontroll över tillgång	17
2.7 Rätt till kontroll över information	18
3 KONSTITUTIONELLT SKYDD FÖR INTEGRITETEN	20
3.1 Integritet i regeringsformen	20
3.2 Motiven till regeringsformen	22
3.3 EU:s rättighetsstadga	23
3.4 Integritetsskydd i europakonventionen	23
4 IPRED	25
4.1 Allmänt om direktivet	25
4.2 Informationsföreläggandeinstitutet	27
4.3 Trafikdata och personuppgiftsskydd	30
4.4 Motiven till implementeringen	31
4.5 Kritik mot implementeringen	34
4.6 Händelser efter implementeringen	36

5	TELEKOMPAKETET	38
5.1	Huvuddragen i nuvarande reglering	38
5.2	Huvudsakligt innehåll i förslaget	40
5.3	Hadopi och medbeslutandeförfarandet	41
5.4	Tvistefrågorna	43
5.5	Kritik mot Telekompaketet	48
6	DATALAGRINGS-DIREKTIVET	51
6.1	Allmänt om direktivet	51
6.2	Innebörden av direktivet	52
6.3	Den svenska implementeringen	54
6.4	Kritik mot direktivet	56
6.5	Datalagring kontra Ipred	59
7	AVSLUTANDE DISKUSSION	62
7.1	Lagring av personlig information	63
7.2	Tillgång till personlig information	66
7.3	Telekompaketet och tillgång	71
7.4	Europakonventionen revisited	74
7.5	Integritetsproblematiken i framtiden	77
	KÄLL- OCH LITTERATURFÖRTECKNING	79
	RÄTTSFALLSFÖRTECKNING	89

Summary

A thorough analysis of several of the privacy issues raised by the Data Retention Directive, IPRED and the Telecoms Package is made in this essay. The regulations are studied in terms of their legal meaning and entailing from a privacy perspective – i.e. if they at all can be said to be problematic from a privacy perspective, and if so in what way. Also the grounds stated in support of each regulation and the criticisms made against them is studied in the essay. The paper concludes with an analysis where the different sides' arguments are discussed from a privacy perspective. The essay begins with two more general chapters where privacy is studied first from a prescriptive normative point of view in which fundamental questions such as what privacy is and why it is worthy of protection is given a couple of possible answers to, and then from a legal descriptive point of view in which the basic legal protection of privacy is presented.

Regarding IPRED it is the extent of the Swedish implementation of the EC Directive which bears that name that has been criticized from a privacy perspective in Sweden. A new legal instrument were introduced by which copyright holders can obtain certain information from other persons, and also ISP's can be forced to disclose already stored data about a subscriber who has an IP address from which a suspected copyright infringement has occurred. The legislature was not obliged to impose a such extensive regulation by the Directive. The grounds given to support the extensive Swedish implementation of IPRED can rightly be questioned and criticized.

The Telecoms Package is a collective term for five EC Directives which primarily regulates infrastructure and competitive issues in the telecom market in the Union. Recently, a frequently mentioned reform of this regulation was adopted, and which also caused major disputes between the governing organs of the union. The political conflict is in the light of the issues raised, and since all Member States also have adopted the ECHR, very odd. The concerns which were raised about the reform are indeed serious, but they have fortunately either never been in question in the legislative process or have been raised against a proposal that has received a great deal of media proliferation but which did not have a broad political support.

The Data Retention Directive is even today a politically very controversial Directive which implies that providers of electronic services must store a variety of telecommunications data for law enforcement purposes. The directive is not yet implemented in Swedish law, but should have been by March 15, 2009. Data stored in accordance with the Data Retention Directive can not be disclosed to copyright holders in accordance with the implementation of IPRED. Data Storage under the Directive could possibly be unlawful under the ECHR. Data Storage in accordance with the directive may however be legitimately questioned from a privacy perspective, and the grounds stated in support of the data retention can be criticized.

Sammanfattning

I uppsatsen görs en grundlig analys av flera av de integritetsskyddsfrågor som aktualiseras av datalagringsdirektivet, Ipred och Telekompaketet. Det redogörs således för vad de respektive regleringarna rent faktiskt medför och innebär rättsligt ur integritetshänseende – dvs. om de över huvud taget kan sägas vara problematiska med hänsyn till en rätt till integritet, och i så fall på vilket sätt. Därefter redogörs för de skäl som har anförts till stöd för respektive reglering samt den kritik som har riktats mot dem. Uppsatsen avslutas med en analys där de olika sidornas argument diskuteras ur ett integritetsperspektiv. Uppsatsen inleds med två allmänna kapitel där integriteten först behandlas ur en preskriptiv normativ synvinkel där grundläggande frågor som vad integritet är och varför det är skyddsvärt ges ett par möjliga svar på, och därefter ur en rättsdogmatisk deskriptiv synvinkel vad gäller det grundläggande rättsliga skydd som finns för den personliga integriteten.

Beträffande Ipred är det omfattningen av den svenska implementeringen av det EG-direktiv som bär denna beteckning som har kritiserats ur ett integritetsperspektiv i Sverige. Ett nytt civilprocessuellt institut infördes, och detta kom att omfatta också internetleverantörer som kan tvingas att lämna ut sedan tidigare lagrade uppgifter om en abonnent som står bakom en IP-adress varifrån ett misstänkt rättighetsintrång tros ha skett. Lagstiftaren var inte tvingad att införa en sådan utsträckt reglering i förhållande till direktivet. De skäl som angavs till stöd för utsträckningen av den svenska implementeringen av Ipred kan med fog kritiseras.

Det s.k. Telekompaketet är ett samlingsnamn för bl.a. fem EG-direktiv som främst reglerar infrastruktur och konkurrensfrågor på telekommarknaden inom unionen. Nyligen antogs en mycket uppmärksam reform av denna reglering, och som också orsakat stora tvister mellan de gemenskapsrättsliga organen. Den politiska striden framstår med hänsyn till vilka frågor den rör, och med hänsyn till att samtliga medlemsstater också har tillträtt europakonventionen, dock som mycket märklig. De farhågor som har rests kring reformen har visserligen varit allvarliga, men har lyckligtvis antingen aldrig varit på tal i lagstiftningsprocessen eller riktat sig mot förslag som fått en stor medial spridning men som inte fått ett särskilt stort politiskt stöd.

Datalagringsdirektivet i sin tur är ett politiskt fortfarande mycket kontroversiellt direktiv som föreskriver att en mängd trafikuppgifter ska lagras av leverantörer för elektroniska tjänster i brottsbekämpande syften. Direktivet är ännu inte implementerat i svensk rätt, men skulle ha varit det senast den 15 mars 2009. Uppgifter lagrade i enlighet med direktivet kommer inte att kunna begäras genom ett informationsföreläggande. Uppgiftslagring enligt datalagringsdirektivet kan möjligen ligga på gränsen för det tillåtna enligt europakonventionen. Uppgiftslagring i enlighet med datalagringsdirektivet kan med fog ifrågasättas ur ett integritetsperspektiv, och också de skäl som har anförts till stöd för uppgiftslagringen kan kritiseras.

Just because you're paranoid doesn't mean they're not after you
Kurt Cobain

Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. Then the 'right to life' served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, – the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession – intangible, as well as tangible.
Samuel D. Warren & Louis D. Brandeis
The Right to Privacy, 1890

Det påstås att den initierades av [...] Samuel D Warren i ilskan över att en societetstidning bevakade hans och hans unga hustrus dyrbara sällskapsliv
SOU 1987:74, s. 45.

Jag kan inte ge någon definition på en elefant, men om jag får se en sådan är jag genast på det klara med att det är en elefant
Citat återgivet av Bengt Lännergren
SvJT 1979, s. 161

Förkortningar

ACTA	Anti-Counterfeiting Trade Agreement. Folkrättslig upphovsrättstraktat som håller på att framförhandlas.
Civilrättsliga sanktionsdirektivet	Se Ipred.
EGD	EG-domstolen, Europeiska unionens domstol.
EGF	EG-fördraget, Fördraget om upprättandet av Europeiska gemenskapen.
EKMR	Europarådets konvention om de mänskliga rättigheterna.
FRA	Försvarets radioanstalt. Svensk myndighet under försvarsdepartementet som bl.a. bedriver signalunderrättelsetjänst.
Ipred	Intellectual Property Rights Enforcement Directive, Europaparlamentets och Rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter, civilrättsliga sanktionsdirektivet.
JO	Justitieombudsmannen.
PuL	Personuppgiftslag (1998:204).
RF	Regeringsformen (1974:152).
SOU	Statens offentliga utredningar.
UrL	Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk.

1 Inledning

Under de senaste två åren har det förts en varierande och vidsträckt debatt i Sverige runt en stor mängd inbördes skiftande rättsområden och förslag på nya rättsliga regleringar som direkt eller indirekt berör olika former av mänsklig kommunikation via tekniska medium. Denna debatt har tenderat att bygga på invändningar som innebär att de vanligen angripna förslagen är integritetskränkande. Debatten har i stor utsträckning också förts på internet eftersom detta medium i samtliga fall berörs mer eller mindre direkt av de kontroversiella normerna. Några av de områden som har figurerat i denna ihållande och mångfacetterade diskussion är således den s.k. FRA-lagen som reglerar svensk signalunderrättelsetjänst för telefoni och datakommunikation, utformningen av den moderna immaterialrätten och framför allt upphovsrätten – och kanske särskilt händelserna kring The Pirate Bay och det s.k. ACTA-avtalet som håller på att förhandlas fram på internationell nivå, den svenska implementeringen av det civilrättsliga sanktionsdirektivet ofta också kallat IPRED eller IPRED-lagen, (det nya) Telekompaketet som bl.a. påstås reglera framtida innehåll på internet, samt omfattande lagring av trafikuppgifter i brottsbekämpande syften enligt det s.k. datalagringsdirektivet.

Den integritetsproblematik som aktualiseras vid samtliga dessa former av regleringar är viktig. Och om inget annat har debatten visat att många människor upplever dessa frågor som angelägna. De normer som har diskuterats och kritiserats befinner sig som synes på olika nivåer; såväl på en helt nationell nivå, som på gemenskapsnivå och på en renodlad internationell nivå. *Det övergripande syftet med denna uppsats* är att göra en grundlig analys av flera av de integritetsskyddsfrågor som aktualiseras av de kritiserade regleringar vilka inte befinner sig på en strikt nationell nivå. Debatten kring The Pirate Bay och alla händelser och omständigheter däromkring, tillsammans med fildelningsdebatten i de delar denna berör utformningen av den moderna immaterialrätten samt ACTA-avtalet bortses därmed från i denna uppsats. Dessa frågor kan inte i första hand sägas handla om integritet. Den i och för sig ur integritetssynpunkt intressanta debatten kring Försvarets radioanstalt samt den av dem bedrivna verksamheten lämnas sålunda också utanför ramarna för denna uppsats.¹

Således ska de aktuella och uppmärksammade regleringar med gemenskapsrättslig anknytning som berör kommunikation i denna uppsats studeras ur ett integritetsperspektiv. Dessa tre områden, som följaktligen har sin grund i Ipred, Telekompaketet och datalagringsdirektivet, reglerar som sagt egentligen inbördes klart skiftande frågor, men har också ett flertal gemensamma

¹ En mycket bra artikel vilken diskuterar bl.a. dessa frågor kring FRA finns dock publicerad i SvJT 2009 s. 519 av Mark Klamberg. Uppsatsens anknytning till ämnet straffrätt har ifrågasatts. Det kan inledningsvis dock ganska kort konstateras att utformningen av implementeringen av Ipred motiverades med att ett alternativ till straffrättsliga åtgärder skulle skapas. De farhågor som har rests kring Telekompaketet har också straffrättsliga anknytningar. Slutligen beträffande datalagringsdirektivet är den straffrättsliga kopplingen genom de syften som anges för upplagringen uppenbara.

hållpunkter med hänsyn till den integritetsproblematik som de aktualiserar. Som det kommer att framgå på ett flertal ställen i uppsatsen är till att börja med okunskapen kring vad de kontroversiella regleringarna går ut på eller innebär i allt för många fall betydande. *Den första mer specifika intentionen med denna uppsats* är därför att utförligt redogöra för vad respektive reglering *faktiskt medför* ur integritetshänseende. Dessa delar av uppsatsen är därför också kanske de allra viktigaste. Beträffande Ipred är det delar av utsträckningen av den svenska implementeringen som har kritiserats, och det är således för denna som ska redogöras för i denna del. Det s.k. datalagringsdirektivet är inte implementerat i svensk rätt ännu. Det är därför istället den kritiserade uppgiftslagring av personlig information som följer av detta direktiv som ska redogöras för. Slutligen avseende det s.k. Telekompaketet är det innehållet i delar av en reform av ett antal EG-direktiv som vanligen går under denna beteckning som har kritiserats, och således ska innehållet i denna reform redogöras för i denna del.

Den andra mer specifika intentionen med denna uppsats är att därefter diskutera innebörden av de nyssnämnda regleringarna ur ett integritetsperspektiv, och analysera de olika sidornas argument. Därför bör på samma sätt de skäl som från officiellt håll har angivits i de kontroversiella delarna studeras och återges. Beträffande Telekompaketet och datalagringsdirektivet ska således redogöras för vad som från gemenskapsrättsligt håll har framförts till stöd för de kontroversiella delarna av denna reglering. Beträffande genomförandet av Ipred är det som redan har nämnts ovan omfattningen av den svenska regleringen som har kritiserats, och i denna del är således lagstiftarens motivering av intresse. För respektive problemområde återges också exempel på innehållet i den kritik som har framförts mot respektive reglering ur integritetshänseende.

Eftersom de ifrågavarande regleringarna har kritiserats med utgångspunkt i att de inte utgör godtagbara inskränkningar i den rätt till personlig integritet som tillkommer alla och envar, och dessa frågor och invändningar dessutom ytterligare ska analyseras i denna uppsats, bör inledningsvis emellertid ett par andra frågor först behandlas. I en text som diskuterar integritet kan den mest grundläggande frågan – vad integritet är – inte förbises. Och för att invändningar som bygger på integritet över huvud taget ska kunna beaktas måste först någonting sägas om vad integritet är för något, och framförallt varför det är eller bör anses vara skyddsvärt. I dessa frågor ska några vanliga uppfattningar återges. Det ska också redogöras för några vanliga uppfattningar i närliggande frågor som om inskränkningar av integriteten alls bör kunna göras, och i så fall under vilka förutsättningar samt vilka skäl som då får väga tyngre. Något kort ska plikttroget på samma sätt sägas om begreppets idéhistoriska bakgrund, likaså om vilket konstitutionellt rättsligt skydd som finns för integriteten i Sverige och Europa.

Ett fåtal mindre frågor som kommer upp i anslutning till de tre studerade rättsområdena kommenteras också i uppsatsen. Således återges beträffande Ipred i ett kort avsnitt ett par viktiga händelser som inträffat efter den svenska implementeringen, vilka är intressanta också i integritetshänseende. Be-

träffande datalagringsdirektivet har det påståtts att det finns ett par gemensamma hållpunkter mellan detta direktiv och Ipred, denna fråga utreds i ett eget avsnitt. Beträffande Telekompaketet redogörs också för den politiska striden i reformarbetet av detta och viktiga bakgrundsfakta till densamma eftersom de integritetsinvändningar som riktats mot reformen av Telekompaketet måste ses i ljuset av dessa. Något sägs slutligen också om de rättsliga implikationer (och komplikationer) de ifrågavarande regleringarna kan medföra ur ett integritetshänseende i anslutning till europakonventionen.

Uppsatsens fokus och frågeställningar påverkar i sedvanlig ordning *den metod som kan användas* (och används). Samtidigt sökes med ljus och lykta efter studenter villiga att skriva examensarbeten med alternativa metoder och perspektiv vid juristutbildningen. Allt annat än sedvanlig rättsdogmatisk metod är dock direkt olämplig att använda i denna uppsats i de delar som innebörden av de rättsområden som ska undersökas ska återges i integritetshänseende, och detsamma gäller för avsnittet om konstitutionellt rättsligt integritetsskydd. I strikt mening begränsar sig den traditionella rättsdogmatiska metoden till uttalanden om gällande rätt. Andra frågor går inte ens att formulera med ett traditionellt rättsdogmatiskt synsätt. För studien av de skäl som har angetts till stöd för de kontroversiella regleringarna och deras utformning har dock sedvanliga juridiska källor använts. Beträffande de invändningar som har riktat sig mot de ifrågavarande regleringarna har detta material dock sällan varit tillräckligt för att ens ge exempel på sådana invändningar som har framförts. I dessa delar har jag istället i första hand använt mig av de största svenska morgontidningarnas tämligen utförliga bevakning av denna diskussion.

Slutligen beträffande det allmänna moralfilosofiska integritetsavsnittet är istället den rättsdogmatiska metoden direkt olämplig.² Som också kommer att nämnas i inledningen till detta kapitel skulle en fullständig översikt över integritetsbegreppet om inget annat bli allt för tids- och utrymmeskrävande för att göras i denna uppsats. Istället har några av de mest citerade och välkända artiklarna där integritetsbegreppet diskuteras använts för att ge ett fåtal exempel på hur man vanligen kan argumentera för en rätt till personlig integritet, samt dess utformning och vilka eventuella begränsningar denna samtidigt bör kunna sägas ha.

Uppsatsens disposition följer i både övergripande och inbördes ordning den frågeställning som har utvecklats ovan, om än de bägge allmänna avsnitten där integriteten behandlas först ur en filosofisk och därefter ur en konstitutionell rättslig synvinkel kommer först. Disposition och sammanhang bör framgå redan av en klart skriven text, och inte genom ständigt bläddrande till innehållsförteckningen för att med hjälp av orimliga hierarkiska rubriker söka klargöra var man som läsare är någonstans (samt vad texten egentligen handlar om). Samtliga kapitel i denna uppsats har därför också avsiktligen

² Detta undantar dock inte att denna i vissa fall ändå används också i sådana frågor. Se exv. direkt under kapitel 2 nedan för den mycket vanliga ”definitionen” av integritet med stöd just i juridiska källor (vilket i förlängningen medför att integritet är skyddsvärt eftersom det har ett rättsligt skydd).

skrivits för att kunna läsas i inbördes fristående ordning. Detta gäller också detta inledningsavsnitt om än det lämpligen inte läses allra sist. Därför redogörs också i respektive kapitel för vad som behandlas däri. Av samma anledning återges i många fall också summariskt vad som har sagts i föregående eller efterkommande avsnitt när det finns gemensamma beröringspunkter. I något fall kan därför också upprepningar av information ske i uppsatsen. Detta är således avsiktligt, och framgår också av sammanhanget. De tre viktigaste områdena i uppsatsen har, om än de kan sägas höra ihop i vissa avseenden, förärats med separata kapitel. Det rör sig trots allt om klart diversifierande rättsområden. Slutligen bör saker vanligen diskuteras i sitt sammanhang. På ett fåtal ställen diskuteras således mindre frågor s.a.s. inne i uppsatsen. De tre problemområdena diskuteras dock i ett sammanhållet avslutande avsnitt eftersom de i detta avseende har fler gemensamma nämnare än skillnader.

Ett par språkliga klargöranden bör avslutningsvis också göras. Det förekommer av naturliga skäl ett flertal mer eller mindre tekniska begrepp i uppsatsen. Förklaringar till de mest komplicerade av dessa ges i noterna. I något enstaka fall har detta inneburit något nedtyngda noter. Eftersom lagstiftningen i dessa fall uppenbarligen inte gjorts teknikneutral har detta dock blivit nödvändigt, eftersom begreppen för många likväl inte är kända.³ Flera av de beteckningar som används i uppsatsen skrivs i många andra sammanhang med VERSALER. Ett sådant bruk genom att exempelvis ständigt behöva skriva IPRED med stora bokstäver tynger dock ned ifrågavärande text väldigt mycket, och även om man anser att något leder till allmänt fördärv finns det bättre sätt att söka visa detta än genom att använda versaler (exempelvis genom en sund och övertygande argumentation istället). Ipred och liknande förkortningar vilka har hunnit bli självständiga akronymer skrivs därför i uppsatsen endast med stor begynnelsebokstav.

På tal om egennamn har det globala datakommunikationsnät som i svenskan vanligen åsyftas med det från början engelska lånordet ”Internet” i sin karaktär av sådant fram tills för ett par år sedan i alla sammanhang också skrivits med Stor Begynnelsebokstav. Internet är idag dock avmystifierat, samt skrivs också i officiella sammanhang allt oftare med liten begynnelsebokstav, och jag ansluter mig härmed till detta bruk. Seden framstår också som särskilt motsägelsefull när den kombineras med svenskans förkärlek till sammansatta ord. Det gamla Televerket är således samtidigt telekombolaget Telia, som Internetleverantören Telia. Slutligen beträffande lagar och direktiv skrivs lagnamn av hävd alltid med små bokstäver, åtminstone i juridiska texter. Samma regel gäller för direktiv. Detta medför således att den skenbara paradoxen i att skriva ”Telekompaketet” med stor begynnelsebokstav och ”datalagringsdirektivet” med liten, är just skenbar.

³ Beträffande noterna används dessa utöver detta huvudsakligen för källhänvisningar samt kommentarer som inte ryms inom uppsatsens frågeställning, och/eller inte tillför sammanhanget något i övrigt (men ändå är så pass intressanta – eller roliga – att de trots detta måste återges i någon form). Liksom denna not således.

En inledning ska slutligen hållas kort, om inget annat för att läsaren inte ska tappa intresset redan i en skrifts första avsnitt.

Således inleds härmed den sista text som jag kommer att producera under mina nio terminer vid juristutbildningen.

2 Integritet

Kritiken mot de föreslagna, och i vissa fall också antagna, rättsregler som ligger i fokus för denna uppsats har huvudsakligen riktat sig mot de allt för stora integritetsintrång som anses bli resultatet av utformningen av denna reglering. I detta, uppsatsens egentliga inledande avsnitt, ska integriteten särskilt behandlas och skärskådas. Till att börja med kan helt kort konstateras att begreppet integritet knappast har en allmänt vedertagen definition. Därutöver utelämnar tämligen ofta kritiker av de rättsregler som behandlas i resten av denna uppsats på vilket sätt de menar att utformningen av denna reglering är integritetskränkande. Därmed förbiser dessa personer vilken ideologisk och/eller filosofisk grund dessa påståenden står på, samt vilken innebörd de till följd därav lägger i begreppet integritet.

Av dessa skäl ska därför integriteten i detta kapitel behandlas ur en preskriptiv normativ synvinkel. Som sagt råder det långt ifrån konsensus om vad paraplybegreppet integritet går ut på. Ämnet har under 1900- och 2000-talet behandlats av otaliga författare, vars skilda meningar om hur begreppet ska förstås i olika grad har medverkat till konceptets utveckling, och påverkat dess innebörd. Detta medför naturligtvis att en något så när fullständig vy över begreppet integritet skulle kräva en inte oansenlig mängd arbete att sammanställa. En sådan komplett översikt skulle därtill inte tillföra den diskussion som förs kring integritet i resten av denna uppsats något. I detta kapitel redogörs således för några vanliga ideologiska grunder för de former av integritet som aktualiseras inom de områden som resten av denna uppsats berör, samt de eventuellt förekommande gränser dessa former av integritet samtidigt anses ha. Detta kapitel gör således inte anspråk på att ge en övergripande eller uttömmande översikt av hur begreppet integritet har behandlats av moderna författare och debattörer, eller dra några generella slutsatser på en sådan grund. Avsikten är istället endast att få ett grepp om, ge exempel på, och närmare undersöka, några av de vanligare definitionerna av, och skälen, gränserna och undantagen till, integriteten.

En definition av integritet som inledningsvis är i det närmaste obligatorisk att nämna är den som bl.a. återges i det tämligen nyutkomna slutbetänkandet *Skyddet av den personliga integriteten* av den s.k. integritetsskyddskommittén. Med denna begreppsförklaring görs en åtskillnad mellan olika former av integritet, främst med ledning av regeringsformens andra kapitel och Europarådets konvention om de mänskliga rättigheterna (EKMR). Man skiljer då mellan en rumslig integritet såsom hemfriden, en materiell integritet såsom äganderätten och egendomsskyddet, kroppslig integritet såsom skyddet för liv och hälsa, personlig integritet i fysisk mening såsom skyddet för den personliga friheten och rörelsefriheten, samt personlig integritet i ideell mening såsom skyddet för privatlivet och personligheten. Denna indelning är på inget sätt ny, den är en typisk svensk utredningsprodukt som går att spåra till många tidigare statliga utredningar och betänkanden där integritet be-

rörts i en eller annan form.⁴ Utöver återgivandet av denna indelning problematiseras och diskuteras tyvärr inte skälen bakom, eller utformningen av, integriteten och dess gränser i integritetsskyddskommitténs betänkande – och detsamma gäller tidigare svenska utredningar.⁵ Således förbises den mest grundläggande frågan; varför vi överhuvudtaget ska ha ett integritetsskydd. Svaret på denna fråga bidrar i förlängningen också till utformningen av integriteten och antyder dess gränser.

2.1 Tidig historik

Redan de gamla grekerna⁶ kan sägas ha haft en uppfattning om ett skydd av det privata. De filosofiska rötterna för dagens vida integritetsbegrepp står således att finna i Aristoteles distinktion mellan den publika sfären, ämnad främst för politisk och annan allmän verksamhet, och den privata sfären, med anknytningar till familjen och hemmet. Två andra, i sammanhanget tidiga, filosofer vilka också brukar sägas ha haft viss betydelse för dagens integritetsbegrepp är John Locke och John Stuart Mill.⁷

Locke återanvände Aristoteles åtskillnad, och sa också bl.a. att människan äger sig själv och sin egen kropp, när äganderätten avhandlades i hans andra uppsats i den anonymt utgivna samlingen *Two Treatises of Government*.⁸ Vad gäller Mill är det främst hans verk *On Liberty* som kan sägas ha haft betydelse för integritetsbegreppet. Mill såg en representativ demokrati som klart fördelaktig i *On Liberty*, samtidigt som dennas makt kraftigt borde begränsas i förhållande till individen och dennes friheter. Mill gjorde en liknande distinktion som Aristoteles och Locke mellan det privata och det publika, där den statliga regleringen enligt Mill främst skulle begränsa sig till den publika sfären, och den privata således var bäst lämpad för individens självstyre.⁹

2.2 Privacy – ett nytt integritetsbegrepp

Den första moderna diskussionen kring personlig integritet brukar tillskrivas Samuel D. Warren och Louis D. Brandeis och deras artikel *The Right to*

⁴ Jfr. SOU 2008:3, s. 64, 340, SOU 1984:54 s. 42.

⁵ Jag återkommer dock till motiveringen till, och skälen bakom, det svenska rättsliga integritetsskyddet i avsnitt 3.2 nedan.

⁶ Efter fyra år vid universitetet har jag äntligen funnit ett ämne som kan inledas med denna – underbara – fras.

⁷ Jfr. DeCew.

⁸ Locke, s. 285ff. Naturligtvis varierar pagineringen efter vilken utgåva man letar i. Äganderätten berörs i vilket fall i kapitel 5 i *Second Treatise*.

⁹ Mill, främst s. 83 – 103, Detsamma gäller för Mill, det är kapitel 4 i *On Liberty* som avses. Argumentationen för en representativ demokrati är naturligtvis än tydligare i *Considerations on Representative Government*, särskilt kapitel 3 däri, s. 238ff. Jfr. Wolff, s. 104f, 117f.

Privacy publicerad i Harvard Law Review den 15 december 1890.¹⁰ I denna artikel drogs gränserna för en ny mänsklig eller medborgerlig rättighet upp – *rätten att få vara ifred*. Artikeln kan sägas ha föranletts av liknande faktorer som de bakom dagens integritetsdebatt; den politiska, ekonomiska och sociala utveckling som skedde under slutet av 1800-talet ansågs av artikelförfattarna medföra ett behov av nya sorters skydd för individen. Dåtidens nya uppfinningar och affärsmetoder möjliggjorde, och orsakade, aldrig tidigare skådade möjligheter till intrång i andras privat- och familjeliv. Warren och Brandeis upplevde särskilt tidningsförlagens, mot den enskilde, aggressivare framtoning och förbättrade fototekniker som särskilt stora hot, och pressen ansågs av artikelförfattarna överskrida de uppenbara gränserna för sed och anständighet i varje riktning.¹¹ De integritetsintrång som också skedde, orsakade enligt Warren och Brandeis dessutom mycket mer psykisk smärta och lidande hos de utsatta än vad som orsakas av ren misshandel.¹² Det fanns således, pga. de nya tiderna, ett nytt skyddsbehov, och detta behov var så starkt att en helt ny typ av rättighet krävdes.

Syftet med Warren och Brandeis artikel var, mot denna bakgrund, att se om den dåtida amerikanska rättsordningen gav utrymme för en princip som skyddade den personliga integriteten. Och om så var fallet, vilken utformning och omfattning detta skydd hade.¹³ Warren och Brandeis tyckte sig kunna skönja en över tiden kontinuerlig utveckling av rätten. Från ett tidigt väldigt torftigt skydd gentemot de grövsta fysiska angreppen på liv och egendom, till ett modernt och utvecklat skydd för liv och person på flera plan inklusive det mentala, och ett omfattande egendomsskydd som också inkluderade immateriella rättigheter. Det var nu dags för nästa steg i denna naturliga utveckling.¹⁴

Warren och Brandeis härledde en rätt till (kontroll över) information om en själv – i vilken mån tankar och känslor ska kommuniceras till andra, och när så görs, rätten att få bestämma i vilken mån och utsträckning dessa ska publiceras – ur en mer generell rätt att få vara ifred. En rätt att få vara ifred som i sin tur kunde härledas ur en större rättighetskälla; rätten till en okränkbar person och personlighet, och rätten till sig själv. Denna rättighet sågs av Warren och Brandeis som den främsta grunden till en rätt till integritet. Äganderätten och immaterialrätten sågs också endast som specialfall av denna rättighet, och de skäl som låg till grund för dessa rättigheter gjorde sig också starkt gällande på det mer grundläggande planet. Rätten till information om en själv, och rätten att få vara ifred, blev därför också närliggande andra grundläggande rättigheter såsom rätten att inte bli angripen eller slagen, fängslad, felaktigt åtalad eller förtalad, eftersom också dessa kunde

¹⁰ Jfr. Lännergren, s. 161, SOU 1987:74, s. 45, DeCew, 1.1.

¹¹ Som kuriosum måste påminnas om citatet från SOU 1987:74 som återgavs just före inledningen.

¹² Warren & Brandeis, s. 193ff.

¹³ Warren & Brandeis, s. 197.

¹⁴ Warren & Brandeis, s. 193ff.

ses som specialfall av rätten till en okränkbar person och personlighet, och rätten till sig själv.¹⁵

De ”nya” rättigheterna gällde gentemot alla och envar, om än argumentationen särskilt tog sikte mot tidningsförlag. Rätten att få vara ifred var dock inte absolut utan relativ. Ett par pragmatiskt valda begränsningar beskrevs därför också i artikeln, samtliga avsedda för det dåvarande största hotet mot den nya friheten – tidningarna. Det mest uppenbara undantaget av dessa var individens möjlighet att med sitt samtycke ge upp sin rätt till integritet.¹⁶ Warren och Brandeis skapade således en mänsklig rätt att få vara ifred, och en rätt till kontroll över information, en informationsintegritet. Denna fann sin grund och motivering främst ur en mer grundläggande rätt till en okränkbar person och personlighet och individens rätt till sig själv. Men också till viss del i ett skyddsbehov, bl.a. eftersom de intrång som skedde, och befarades ske, orsakade människor (mental) smärta och skador.

2.3 Samtida integritetsbegrepp

Spår och liknande drag i många av de tankar som återfinns i Warren och Brandeis artikel hittas också hos mer nutida författare. Innan den samtida synen på integritet undersöks bör dock innebörden i, och skillnaden mellan, att något anses ha ett etiskt egenvärde, och ett instrumentellt värde i förhållande till ett annat värde, i praktiskt argumentation framhållas. Att något har ett etiskt egenvärde betyder att det är värdefullt i sig självt och inte kan motiveras ytterligare. Detta till skillnad från när något har ett instrumentellt värde, då värdet är beroende av att något annat värde befrämjas. Det blir således med nödvändighet vid praktiskt argumentation ibland fråga om en cirkelargumentation, lösningen på det ifrågakvarande problemet är etiskt riktigt och motiverat i sig självt.¹⁷

Redan här kan således en del problem anas. Tämligen ofta anses nämligen rätten till en personlig integritet ha ett etiskt egenvärde, om än det inte är fråga om någon absolut rättighet. När integriteten inte är instrumentell i förhållande till ett annat värde försvårar detta också möjligheten att med hjälp av andra värden och riktlinjer dra upp gränserna för integriteten, och ge definitiva utslag i eventuella intressekonflikter med andra värden. Gemensamt för samtliga teorier om en personlig rätt till integritet är att de i någon mening ansluter till läran om naturliga rättigheter, vilken samtidigt brukar sägas bygga på liberala ideal om individens frihet.¹⁸ Samma problem som har antytts för ett rättfärdigande av en individs rätt till integritet gäller de facto över huvud taget för alla mänskliga rättigheter. Rättigheterna anses vara grundläggande, elementära, fundamentala eller axiomatiska. Det finns inte

¹⁵ Jfr. Warren & Brandeis, s. 196, 199 – 205, 213.

¹⁶ Warren & Brandeis, s. 213f, 218.

¹⁷ Jfr. Dahlman, s. 27f. En utilitarist skulle exempelvis säga att anledningen till att samhällsnyttan bör maximeras i samhället är för att det bör vara så.

¹⁸ Jfr. Dahlman, s. 49f.

något mer grundläggande man kan åberopa till stöd för dem. Det är samtidigt väldigt problematiskt att fastställa vilka rättigheter som finns.¹⁹

En uppdelning mellan både förespråkare och motståndare till integritetsbegreppet kan göras i två kategorier; reduktionister och koherentister. *Reduktionister* härleder all integritetsproblematik till, och i vissa fall löser också sådana frågor med hjälp av, andra mer grundläggande och (redan) erkända rättigheter. En renodlad reduktionist ser därför aldrig integritet som något som har ett etiskt egenvärde. Motståndare till integritet som begrepp kan generellt hänföras till denna grupp, eftersom de naturligtvis inte heller ser något etiskt egenvärde i integritet. Enligt vissa reduktionister förstås å andra sidan integritetsfrågor bättre exempelvis i ljuset av en större rätt till frihet för individen, och integritet har då heller inte ett (helt) fristående egenvärde. Andra reduktionister menar att alla integritetsfrågor kan ses som en fråga om äganderättens utsträckning. *Koherentister* erkänner med nödvändighet en rätt till integritet i en eller annan form, och härleder oftast inte heller denna rätt till andra rättigheter eller mer grundläggande begrepp. Många av förespråkarna för integritet hör således hemma i denna grupp, och tämligen ofta har integriteten också sitt etiska egenvärde som enda motivering. Den närmare utformningen och synen på integritet kan dock variera starkt mellan olika förespråkare också inom denna grupp.²⁰

2.4 Frihet och andra rättigheter

Ett flertal huvudspår kan naturligtvis identifieras beträffande den samtida synen på en rätt till personlig integritet (dvs. definitionerna av, skälen bakom samt eventuellt förekommande gränser och undantag till densamma). Ett par exempel på sådana synsätt ska således redogöras för i den återstående delen av detta kapitel. Integritetsbegreppet ligger i sin karaktär av medborgerlig rättighet redan genom detta förhållande nära liberalismen och i förlängningen dess frihetsbegrepp. En författare som således uttryckligen har utvecklat, definierat och argumenterat för en rätt till personlig integritet utifrån ett sådant perspektiv är Robert B. Hallborg, Jr. Enligt Hallborg kan en rätt till personlig integritet i sig delas upp i två delar; en ”konstitutionell rätt till integritet” och en ”moralisk rätt till integritet”. Uppdelningen har trots sina beteckningar emellertid inget att göra med ett rättsligt eller konstitutionellt skydd för integriteten. *Den konstitutionella rätten till integritet* handlar istället om individens rätt att inte bli övervakad av *staten* när individen befinner sig i sin enskildhet, vilket kontrasteras mot *den moraliska rätten till integritet* som handlar om individens rätt att inte bli observerad av *andra individer* utan samtycke i den privata sfären.²¹

Dessa bägge begrepp härleder Hallborg i sin tur ur frihetsprinciper vilka i sig sägs ha sitt ursprung i permanenta värden som återfinns i liberala, demo-

¹⁹ Se exv. Wolff, s. 115f.

²⁰ Jfr. Moore 2008, s. 412, DeCew, 1.3, 2.3.

²¹ Hallborg, Jr., s. 210 – 218.

kratiska samhällen (vad nu detta innebär). En generell rätt till frihet som således enligt Hallborg bygger på ett sådant permanent värde säger att staten inte har rätt att beröva, lägga sig i eller begränsa människors friheter utan goda skäl. Ur denna generella rätt till frihet härleds därefter mer specifika frihetsprinciper, vilka används till grund för de bägge slagen av en rätt till personlig integritet. Den konstitutionella rätten till integritet finner enligt Hallborg därför sitt stöd i en frihetsprincip som säger att när alla andra omständigheter är desamma, så ju större den föreslagna begränsningen av ett frihetsintresse är, desto större blir också den motiveringsbördan som förespråkaren av denna inskränkning måste uppfylla. Principen medför därför bl.a. att en särskild omfattning eller kvantitet av en frihetsinskränkning är moraliskt godtagbar endast om förespråkaren (staten) kan ge en motivering som står i proportion till (hela) omfattningen av denna frihetsinskränkning. Man måste således också ta hänsyn till eventuellt tidigare utförda inskränkningar av integriteten med denna teori. Den moraliska rätten till integritet härleds ur en mycket liknande frihetsprincip (vilken i sin tur också har härletts ur den mer allmänna frihetsprincipen), som säger att när andra omständigheter är lika, ska, när frihetsintressen står mot varandra, den av dem som skadar friheten mest bära motiveringsbördan.²²

Judith Jarvis Thomson är en inom området mycket omtalad författare som har ett helt annat synsätt än Hallborg. Hon ser den personliga integriteten som ett kluster av frågor och rättigheter som inte är distinkt, utan istället alltid skär andra kluster av rättigheter; särskilt äganderätten och rätten till sin egen person. Thomson ser således rätten till personlig integritet som möjlig att alltid härleda till dessa andra (redan erkända) rättigheter, och samtliga integritetsfrågor och integritetsproblem förstås och löses därför bättre i ljuset av dessa. Hon understryker också att hennes poäng främst är att man kan sägas ha en rätt till personlig integritet *för att* man har dessa andra rättigheter, och att det således egentligen alltid är dessa som aktualiseras vid alla former av integritetsproblematik. Uttryckt på ett annat sätt finns det enligt Thomsons synsätt ingen *rätt* till personlig integritet, det finns endast ett kluster av rättigheter som lika gärna kan kallas för personlig integritet, men de saknar gemensam grund – eftersom det egentligen är fråga om andra sorters rättigheter.²³

Både Hallborg och Thomson är med den uppdelning som gjordes i föregående avsnitt naturligtvis typiska reduktionister. Beträffande Hallborgs argumentation kring en rätt till personlig integritet kan ett par allmänna uppenbara begränsningar nämnas. Till att börja med måste det liberala frihetsbegreppet som sådant godtas, och i den form och mening som Hallborg klär det i. Därtill är de bägge bakomliggande frihetsprinciperna till den uppdelning av rätten till personlig integritet som Hallborg gör inte särskilt lämpliga att tillämpa vid intressekonflikter (framförallt är de inte så användbara som det framställs). Frihetsinskränkningar ska vägas mot varandra. Frihet som begrepp definieras dock inte, och det är minst sagt svårt att s.a.s. uppskatta omfattningen av en frihetsinskränkning i någon egentlig mening.

²² Hallborg, Jr., s. 175f, 183f, 210 – 218.

²³ Thomson, främst s. 306, 310ff.

Beträffande Thomson kan konstateras att liknande invändningar som hon implicit riktar mot ett integritetskoncept kan riktas mot de bågge andra ”kluster” vilka hon menar att integritet s.a.s. egentligen består i. Varken äganderätten (eg. rätten till ägande) eller rätten till sin egen person definieras, avgränsas eller ges en motivering till varför dessa rättigheter i sin tur bör finnas eller hur dessa ser ut. Poängen med Thomsons artikel är uttryckligen att integritetsproblematiken alltid kan lösas med hjälp av andra rättigheter och att integritet därför också alltid kan härledas till dessa andra principer. Kontentan av detta är att integritet ges ett nytt namn (eller två) – inget mer. Inga fler problem kan lösas, och när dessa bågge andra rättigheter därtill inte heller preciseras mer ingående blir konceptet än mer svåränvänt.

Ett par ytterligare bra invändningar gentemot Thomsons resonemang framfördes kort efter att den artikel vari dessas framfördes publicerades. Således har också sagts att den viktiga kärnan i integritetsproblematiken lätt förbises när resonemang enbart förs med exempel med pinsamma uppgifter eller liknande. De grundläggande intressen som integriteten skyddar är inte heller överensstämmande med äganderätten eller rätten till sin egen person vilket enkelt går att visa med exempel där de flesta skulle anse att en persons rätt till integritet kränkts, men där dessa andra rättigheter samtidigt inte kan sägas överlappa.²⁴ Det har också framförts att man med Thomsons form av reduktionism får problem vid att avgöra frågor som elektronisk övervakning eller intressekonflikter såsom mellan tryckfrihet och en rätt till personlig integritet med hjälp av äganderättsprinciper.²⁵

2.5 Människlig värdighet och intimitet

Ett annat sätt att rättfärdiga en individuell rätt till integritet är att härleda denna rätt ur en rätt till mänsklig värdighet. Denna rätt till mänsklig värdighet får då samtidigt det yttersta etiska egenvärdet. Warren och Brandeis kan sägas främst ha tillhört denna kategori eftersom de som sagt härledde rätten till kontroll över information ur en större rätt att få vara ifred, vilken i sin tur härleddes ur den grundläggande rätten till en okränkbar person och personlighet, rätten till sig själv. Edward J. Bloustein är en modern författare som också försvarat denna linje, och ytterligare utvecklade denna grundläggande rättighet som skyddas av, och rättfärdigar, en rätt till integritet. Enligt Bloustein är rätten till en okränkbar person och personlighet det som definierar människans själva väsen, och inkluderar hennes individuella värdighet och integritet, personliga autonomi och självständighet. Intrång i den personliga integriteten förstås således bäst som en skymf mot den mänskliga värdigheten.²⁶ En liknande motivering till den enskildes rätt till integritet har framförts av JO Hans-Gunnar Axberger.²⁷ Den svenska lagstiftarens syn på rät-

²⁴ Jfr. Rachels.

²⁵ Jfr. Scanlon.

²⁶ Bloustein, främst s. 971 – 981, 1002f.

²⁷ Axberger, s. 481.

ten till integritet kommer att beröras mer utförligt i kapitel 3 nedan. Redan i detta sammanhang kan dock nämnas att man i vissa lagstiftningsärenden har betonat värdet av den personliga integriteten med hänvisning till just människovärdet.²⁸

Intimitet och integritet kan språkligt i många fall sägas ligga nära varandra. Exempelvis har juristen Robert S. Gerstein således argumenterat för att en rätt till personlig integritet är nödvändig för att möjligheten till intimitet i vid bemärkelse annars skulle omöjliggöras. En respekt för den personliga integriteten ger individen en möjlighet till kontroll över sig själv, kontroll över vem som vet vad, samt vem som har tillgång till individen. Detta ger i sin tur individen en större möjlighet till kontroll över sitt beteende gentemot andra människor och möjlighet till kontroll över, och upprätthållandet av, olika sociala relationer. Utan denna kontroll skulle intima relationer och begrepp som respekt, kärlek, vänskap och förtroende försvåras eller omöjliggöras. Möjligheten till intima relationer och interaktioner med andra människor är nödvändigt för spontanitet och utevaro av skam. Den personliga integriteten har med detta sätt att argumentera således främst ett instrumentellt värde i förhållande till värdet av en möjlighet till intimitet.²⁹

Argumentation på det förstnämnda sättet kan faktiskt sägas vara ett fall av koherens. Rätten till en personlig integritet är visserligen instrumentell i förhållande till ett annat värde. Men detta andra begrepp, vilket i sin tur anses ha ett etiskt egenvärde, är så snarlikt det första, att det i praktiken blir fråga om samma sak. I Blousteins fall består till och med den mänskliga värdigheten bl.a. i en rätt att inte få sin integritet kränkt, och en kränkning av den mänskliga värdigheten såsom den framställs också i övrigt gör föreställningen svår att få ett grepp om. En argumentation på det sistnämnda sättet, på sådana premisser, blir lätt svävande och samtidigt problematisk. Man kan fråga sig om radikala skillnader i folks sociala relationer rent faktiskt skulle uppstå om individernas rätt till integritet inte skyddades och upprätthölls, och vilket stöd det i så fall skulle finnas för detta.

2.6 Rätt till kontroll över tillgång

Ytterligare ett sätt att karaktärisera och definiera den personliga integriteten är att som exempelvis Ruth Gavison eller Adam Moore se det som en fråga om kontroll över tillgång till kroppar, platser och information. Det finns naturligtvis inga skarpa gränser mellan olika synsätt, men också med detta perspektiv på integriteten ges individen en exklusiv rätt till makt och kontroll över sin egen värld och tillvaro, och får en rätt till skydd från oönskad tillgång från andra. Det blir således en fråga om begränsad tillgänglighet, och individen har fullständig integritet när den är helt oåtkomlig för andra.

²⁸ Exempel på när detta har skett ska ha varit i samband med ändringar av rätten till skadeståndersättning för ideella skador samt vid införandet av lagen (2006:351) om genetisk integritet, se Reimers, s. 449.

²⁹ Gerstein.

Integriteten är värdefull eftersom individer som inte får en viss nivå av kontroll över tillgång annars kommer att lida på olika sätt. En rätt till integritet, liksom utbildning, hälsa och att upprätthålla sociala relationer är enligt ett sådant synsätt en essentiell del av människans välbefinnande.³⁰

2.7 Rätt till kontroll över information

Slutligen återfinns Warren och Brandeis sätt att se på integriteten som en rätt till kontroll över information också idag.³¹ Ett bra tämligen samtida försvaret och utveckling av denna linje återfinns i William Parents artikel *Privacy, Morality, and the Law* från 1983. Synen på integriteten i denna artikel påminner också en del om den som beskrevs i föregående avsnitt. Parent ger en helt deskriptiv definition av den personliga integriteten, och ser den som (en rätt till) ett tillstånd där odokumenterad personlig information inte är känd eller innehas av andra personer. Personlig information illustreras i sin tur som fakta individen normalt sett inte vill avslöja till andra såsom hälsa, lön, vikt, sexuell läggning et cetera.³²

Parent är mycket kritisk till ett par andra författares instrumentella argument till stöd för (och i något fall mot) integritet,³³ men framför å sin sida ett par instrumentella argument till stöd för varför en rätt till personlig integritet ska erkännas, samt dennas utsträckning. Parents främsta skäl till varför en rätt till integritet ska erkännas är den skada som sådana intrång annars orsakas, och upplevs av, individen. Detta argument känns också igen från Warren och Brandeis artikel. Därtill framhävs att så länge vi lever i ett samhälle där det finns fördomar och intolerans mot minsta avvikelse hos individen och där ingen vill bli skrattad åt eller bli gjord till åtlöje, samt där de flesta av oss bär på en övertygelse om att det finns uppgifter om oss själva som andra människor, särskilt främlingar och tillfälligt bekanta, inte har rätt att få veta, bör en sådan rättighet också tillerkännas individen. Parent framhåller även att de som motarbetar och motsätter sig en rätt till personlig integritet samtidigt bryter mot distinkta liberala principer om respekt för individen och personen.³⁴ Parent framhåller också att individers strävan efter en rätt till integritet i de flesta fall är helt oskyldig, och inte betyder att man är ute efter att dölja något eller skada någon, samt att rätten inte är absolut, utan att försvarbara undantag förekommer.³⁵

Slutligen definierar Parent sex frågor eller kriterier för att avgöra om ett försvarbart undantag till rätten till integritet föreligger eller inte. De saker

³⁰ Jfr. Gavison, Moore 2003, Moore 2008.

³¹ Således avser jag *inte* hur Warren och Brandeis *rättfärdigade* denna rätt. En modern variant av denna linje återgavs i avsnitt 2.5 ovan.

³² Parent 1983a, s. 269f. Jfr. Moore 2003, s. 215. Parent anför dock också argument till stöd för varför man har rätt detta tillstånd (således är det enbart definitionen i sig som kan sägas vara deskriptiv).

³³ Parent 1983a, s. 275.

³⁴ Jfr. Parent 1983a, s. 276f.

³⁵ Parent 1983a, s. 277f.

man enligt Parent således ska ta ställning till är; (1) i vilket syfte, eller av vilken anledning, den personliga informationen eftersöks och används, (2) om detta syfte är legitimt och viktigt, (3) om den kunskap som inhämtas genom integritetsintrånget är relevant för att legitimera syftet, (4) om integritetsintrånget är det enda, eller minst ingripande, sättet att få denna kunskap, (5) vilka begränsningar och förebyggande åtgärder som finns i de integritetskränkande förfaranden som avses att användas, samt (6) vilket skydd kunskapen får när den väl är inhämtad.³⁶

Med den tidigare uppdelningen mellan reduktionister och koherentister är Parent reduktionist i den meningen att motiveringen till varför en rätt till integritet ska tillerkännas individen inte uteslutande finner sin motivering i sig självt. Samtidigt reduceras inte integritetsbegreppet fullständigt till andra allt för diffusa rättigheter. Ett par invändningar som har riktats mot Parents definition och försvar av integriteten kan också återges. Således har framförts att med Parents definition utesluts efterkommande användning av personlig information från integritetsbegreppet eftersom den ifrågavarande personliga informationen då kan sägas vara dokumenterad och känd av andra personer. Integritetsproblematik måste kunna sägas finnas också på denna nivå.³⁷ I en artikel som kom en kort tid efter hans första undantog Parent uttryckligen publik eller allmänt känd information från sin definition av integritet (vilket i förlängningen således innebär bl.a. att allmänt känd information aldrig kan bli föremål för integritetsproblematik enligt Parents synsätt).³⁸ Det var möjligen svårt att konstruera eller föreställa sig realistiska situationer där man skulle kunna säga att integritetsproblematik aktualiseras också under sådana förutsättningar som Parent undantog från sin definition när artiklarna skrevs 1983. Förhållandet har naturligtvis dock i efterhand kritiserats, bl.a. utifrån att allmän övervakning svårligen omfattas av Parents definition i inskränkt mening.³⁹

Med detta sagt, sätter Parents definition och framförallt försvar av integriteten fingret på flera av de kriterier och egenskaper de flesta torde förknippa med en rätt till integritet. Argumenten och kriterierna passar också bra som utgångspunkt för den integritetsproblematik som aktualiseras inom de områden som resten av denna uppsats berör. De brister som kan påvisas i Parents inskränkta definition av integritet är också väldigt lätta att komma runt. Synen på integritet som en rätt till kontroll över information används därför också som utgångspunkt i den avslutande diskussionen i denna uppsats.

³⁶ Parent 1983a, s. 280f.

³⁷ Moore 2008, s. 416f.

³⁸ Parent 1983b, s. 307ff.

³⁹ Se exv. Nissenbaum, s. 580.

3 Konstitutionellt skydd för integriteten

Något kort bör pliktstroget också nämnas om det grundläggande rättsliga integritetsskyddet. I detta kapitel ska därför integriteten behandlas ur en främst rättsdogmatisk deskriptiv synvinkel i fråga om grundläggande rättsregler som skyddar den privata sfären vilka är relevanta för svenska förhållanden. Således kommer utsträckningen av den personliga integriteten i dessa regler att återges, samt i förekommande fall skäl bakom utformningen och utsträckningen av dem. Någon egentlig definition av begreppet personlig integritet finns inte i svensk lagstiftning. Inte heller finns det något konstitutionellt, rättsligt bindande, *allmänt* integritetsskydd i svensk rätt. Med detta sagt, finns det ändå bestämmelser som tar sikte på den personliga integriteten i regeringsformen (RF).⁴⁰ I detta sammanhang ska naturligtvis inte heller Europarådets konvention om de mänskliga rättigheterna eller EU:s rättighetsstadga glömmas bort.

3.1 Integritet i regeringsformen

Av 1 kap. 2 § 4 st. RF framgår till att börja med att det allmänna ska värna om den enskildes privat- och familjeliv. Denna bestämmelse ger dock inte individen något faktiskt integritetsskydd. 1 kap. 2 § RF är endast ett s.k. målsättningsstadgande, vilket innebär att det ”inte [är] fråga om en rättsligt bindande regel”, utan att bestämmelsen enbart ”ger uttryck för vissa särskilt viktiga principer för samhällsverksamhetens inriktning”, samt att ”[s]tadgandets främsta funktion är att åläggas det allmänna att positivt verka för att de ifrågakvarande målsättningarna i största möjliga utsträckning förverkligas”.⁴¹

Vissa delar av integriteten behandlas utöver detta målsättningsstadgande i den s.k. rättighetskatalogen i 2 kap. RF. Åsikterna om vilket skydd rättighetskatalogen egentligen erbjuder är dock många. Tämmligen ofta framförs den i svensk juridisk (för att inte säga politisk) tradition starka oviljan mot att ge individen en juridiskt skyddad rättighetssfär, som förklaring till de brister som kan påvisas.⁴² Rättighetskatalogen skyddar som bekant endast undersåten gentemot statsmakten, och detta genom att begränsa dennas normgivningsmakt. Rättstillämpande och myndighetsutövande organ får därtill endast undvika att tillämpa lagar och förordningar som står i strid med rättighetskatalogen om dessa tillkommit genom ett uppenbart fel jämte 11 kap. 14 § RF, och en skadeståndstalan gentemot staten (eller någon annan för den delen) kan inte grundas direkt på en överträdelse av 2 kap. RF.

⁴⁰ Se också Axberger, s. 470f och Reimers, s. 435f.

⁴¹ Prop. 2001/02:72, s. 15. Se också SOU 2008:3, s. 96ff.

⁴² Jfr. Axberger, s. 468f. Se också Reimers, s. 448.

Bestämmelserna i 2 kap. RF medför således enbart en negativ förpliktelse för staten, genom att blott reglera lagstiftarens möjlighet att begränsa fri- och rättigheterna.⁴³

Lagstiftarens vanligaste definition av eller syn på integriteten återgavs i början av avsnitt 2 ovan. Samtliga aspekter av denna indelning återfinns också i regeringsformens rättighetskatalog. De olika sådana typer av integritet är dock utspridda i flera av rättighetskatalogens bestämmelser. Således skyddas delar av den *kroppsliga integriteten* genom förbudet mot dödsstraff i 2 kap. 4 § RF, förbudet mot kroppsstraff, tortyr och medicinsk påverkan i syfte att framtvunga eller hindra yttranden i 2 kap. 5 § RF, samt genom förbudet mot påtvingat kroppsligt ingrepp också i annat sammanhang i 2 kap. 6 § RF. Delar av den *rumsliga integriteten* skyddas genom förbudet mot husrannsakan i 2 kap. 6 § RF, och delar av den *personliga integriteten i fysisk mening* genom förbudet mot kroppsvisitation, också det i 2 kap. 6 § RF. Slutligen skyddas delar av den *personliga integriteten i ideell mening* genom förbudet mot undersökning av brev eller annan förtrolig försändelse, mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande i 2 kap. 6 § RF, genom förbudet mot åsiktsregistrering enbart på grund av politisk åskådning i 2 kap. 3 § 1 st. RF, samt slutligen vissa personliga uppgifter som registreras med hjälp av automatisk databehandling genom det säregna stadgandet i 2 kap. 3 § 2 st. RF.⁴⁴

De frågeställningar kring integritet som resten av denna uppsats tangerar är således främst de som huvudsakligen åsyftas i slutet av 2 kap. 6 §, samt 2 kap. 3 § 2 st. RF. Redan av de skäl som återgavs ovan är det integritetsskydd som följer av dessa bägge bestämmelser dock relativt svagt. Utöver detta framgår det av 2 kap. 12 § RF att det skydd som ges i 6 § får begränsas genom lag under vissa närmare angivna förutsättningar, och således inte är absolut. 2 kap. 3 § 2 st. RF föreskriver å sin sida mer specifikt att varje medborgare, i den utsträckning som närmare anges i lag, ska skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatisk databehandling. Denna bestämmelse ger följaktligen individen ett än mer begränsat integritetsskydd, eftersom den inte ens – till skillnad från bestämmelserna i resten av 2 kap. RF – begränsar lagstiftarens normgivningsmakt, utan enbart är en vanlig normgivningsregel. Bestämmelsen kan därför heller aldrig tillämpas av rättstillämpande och myndighetsutövande organ.⁴⁵

Vad gäller den positiva utsträckningen av dessa bägge bestämmelser, och detta kan sägas gälla också för de övriga fri- och rättigheterna, utvecklas inte denna nämnvärt i förarbetena. På det sätt bestämmelserna därtill är utformade, och på vilket sätt de därför också används, finns det inte heller

⁴³ Reimers, s. 436, 443f. Jfr. SOU 2008:3, s. 97 – 105.

⁴⁴ Jfr. SOU 2008:3, s. 99 – 105, 113ff, SOU 1984:54, s. 42.

⁴⁵ Bestämmelsen följs dock. Integritetsskyddande lagar som kan ses som uttryck av 2 kap. 3 § 2 st. RF är bl.a. personuppgiftslagen och lagen om elektronisk kommunikation. Naturligtvis reglerar en hel del bestämmelser i sekretesslagen också sådana frågor. Se också SOU 2008:3, s. 102, 105ff, 113ff och Reimers, s. 437.

någon ”levande” utveckling av dem i rättspraxis.⁴⁶ Det kan tilläggas att integritetsskyddskommittén, tillsammans med grundlagsutredningen, kritiserar lagstiftaren för att i frånvaron av rättsligt verkande konstitutionella bestämmelser, som generellt tar sikte på ett personligt integritetsskydd, inte lägger tillräcklig vikt vid integritetsfrågor vid ny lagstiftning inom områden där dessa aspekter berörs. Integritetsskyddskommittén föreslår därför en utökning av skyddet för den personliga integriteten i 2 kap. 6 § RF till att innefatta ett skydd mot intrång som sker i hemlighet eller utan samtycke, och som i betydande mån innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Grundlagsutredningen instämmer även i denna propå. Regeringen torde dock inte ha tagit ställning i saken ännu, och om några ändringar ska ske inom överskådlig tid börjar det snart bli bråttom med ett år tills nästa riksdagsval.⁴⁷

3.2 Motiven till regeringsformen

Slutligen gällande regeringsformen kan tämligen kort konstateras att motiven till integritetsskyddet inte utvecklats beaktansvärt i förarbetena. Integriteten finner inte sin motivering i ett eget skyddsintresse, den är inte heller direkt kopplad till några ideal om individens ovedersägliga och okränkbara rättigheter, och integriteten kan därför inte heller sägas ha ett etiskt egenvärde.⁴⁸ De skäl vilka jag redan har nämnt ovan brukar anföras som förklaring också till detta – den av tradition starka svenska oviljan att ge individen ett rättighetsskydd, underförstått gentemot staten. Andra värden anses istället vara betydligt viktigare i Sverige. Den princip som kanske understryks allra mest i förarbetena till 1976 års reform av regeringsformens rättighetskatalog är värdet av ett fritt och demokratiskt samhälle, där den jämförelsevis utomordentligt starka tryckfriheten och offentlighetsprincipen särskilt sticker ut. Tryckfriheten och offentlighetsprincipen i sin tur, tillsammans med skyddet av den fria åsiktsbildningen, motiveras och ses som uttryck av samhällsnyttan och just skyddet av ett fritt och demokratiskt samhälle. Individens rättighetssfär kan inte sättas före det allmännas bästa, och individens rättigheter finner också sitt stöd i det allmännas bästa. Respekten för individen och en personlig integritet har därför främst ett instrumentellt värde i förhållande till stärkandet av demokratin och den fria åsiktsbildningen, och de grundläggande fri- och rättigheterna ger uttryck för värderingar som oupplösligen är förbundna med demokratins idéer.⁴⁹

⁴⁶ 11 kap. 14 § RF kan inte sägas vara någon större drivkraft för en levande svensk konstitution. Det kan tilläggas att bestämmelsen i 2 kap. 3 § 2 st. RF tillkom 1988 med syftet att grundlagsfästa och ytterligare förstärka delar av integritetsskyddet, men att ett par remissinstanser av allmänmotiveringen att döma redan då uttryckte ett visst missnöje över att bestämmelsen är ”för snäv och intetsägande”, samt att ”[d]e ser det som en brist att den föreslagna grundlagsregeln inte stakar ut en skyddad sfär”, jfr. prop. 1987/88:57, s. 9ff.

⁴⁷ SOU 2008:3, s. 187ff, 255 – 282, SOU 2008:125, del 1 s. 473ff.

⁴⁸ Jfr. prop. 1975/76:209, s. 43ff, 51ff, 72f, 127ff. Se dock vad som sades i avsnitt 2.5 ovan om vad lagstiftaren i vissa fall på lagnivå motiverat integritet med.

⁴⁹ Axberger, s. 468ff, Reimers, s. 447ff. Jfr. prop. 1975/76:209, s. 43ff, 51ff, 72f, 127ff.

3.3 EU:s rättighetsstadga

Regleringen av fri- och rättigheter i RF kompletteras som sagt också av EKMR samt EU:s rättighetsstadga. Den sistnämnda har än så länge fortfarande endast karaktär av politiskt åtagande från medlemsstaterna. Den kommer dock, när Lissabonfördraget träder ikraft, att få en större betydelse också för svenskt vidkommande avseende rättighetsskydd, eftersom den då kommer att bli rättsligt bindande. Olika delar av integriteten skyddas och behandlas i ett par bestämmelser i stadgan, och över huvud taget överlappar rättigheterna i stadgan stora delar av dem som skyddas också i EKMR.⁵⁰ Eftersom de rättigheter som ges än så länge inte har prövats eller utvecklats av EG-domstolen, hänvisas dock till integritetsskyddskommitténs slutbetänkande avseende den närmare utformningen och utsträckningen av integritetsskyddet i EU:s rättighetsstadga.⁵¹

3.4 Integritetsskydd i europakonventionen

EKMR har däremot varit en integrerad del av den svenska rättsordningen sedan 1994, när konventionen inkorporerades på lagnivå samt bestämmelsen innebärande att lagar eller andra föreskrifter inte får meddelas i strid mot densamma infördes i 2 kap. 23 § RF. Det kan tilläggas att lagprövningsregeln i 11 kap. 14 § RF är tillämplig också gentemot bestämmelser som strider mot EKMR.⁵² EKMR innehåller ett flertal bestämmelser om mänskliga rättigheter som kan sägas omfatta ett skydd av den enskildes rätt till integritet. Företrädesvis är det dock artikel 8 som integritetsskyddet utgår från. I artikel 8.1 föreskrivs tämligen kort att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rätten till privatliv är dock inte absolut, utan inskränkningar i rättigheterna får ske under vissa förutsättningar i enlighet med artikel 8.2. För att en inskränkning ska vara tillåten måste den således ske med stöd i lag och vara nödvändig i ett demokratiskt samhälle. Därtill måste inskränkningen vara ägnad att tillgodose något uppräknat enskilt eller allmänt intresse, såsom statens eller den allmänna säkerheten, landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral, eller för att skydda andra personers fri- och rättigheter.⁵³

Till skillnad från vad man kan säga om 2 kap. RF är rättigheterna (och undantagen till dem) i EKMR väl utvecklade och fastlagda i Europadomstolens praxis. Rättigheterna som följer av artikel 8 gäller därtill inte enbart gentemot staten, utan bestämmelsen ställer också krav på skydd visavi andra

⁵⁰ Jfr. SOU 2008:3, s. 71, 73.

⁵¹ EU:s rättighetsstadga behandlas huvudsakligen på s. 72 – 74 i SOU 2008:3.

⁵² Prop. 1993/94:117, s. 36, 53f, SOU 2008:3, s. 92. När EKMR inkorporerades ansåg lagstiftaren att svensk rätt redan uppfyllde samtliga krav konventionen ställer. Så har ända sedan dess enligt de flesta dock inte ansetts varit fallet. För några samtida exempel på var det brister någonstans, se Abrahamsson, s. 432f och Munck, s. 505.

⁵³ Jfr. SOU 2008:3, s. 72, 82ff.

individer.⁵⁴ Den positiva utsträckningen av det skydd för privatlivet som ges av artikel 8 är därför också betydligt mer mångskiftande och omfattande än vad en första anblick kan ge sken av. Utsträckningen av integritetsskyddet i artikeln i förhållande till vad man enligt svensk rättstradition brukar kalla den personliga integriteten i ideell mening utreds därför lämpligt nog också utförligt i integritetsskyddskommitténs slutbetänkande, med särskild fokus på insamling och offentliggörande av information och uppgifter om den enskilde.⁵⁵ Det är dessa aspekter av det integritetsskydd som följer av artikel 8 EKMR som nu också kort ska återges. Artikel 8 innefattar således bl.a. en rätt att bli lämnad ifred, ett tämligen långtgående skydd för hemmet och den enskildes korrespondens, samt ställer slutligen krav i förhållande till information om privata förhållanden och behandlingen av personuppgifter.

Rätten att bli lämnad ifred enligt artikel 8 är ett skydd mot närgången uppmärksamhet, och innefattar ett skydd mot att bli fotograferad eller avlyssnad, samt ett skydd mot att foton, filmer eller ljudinspelningar av privat natur används för ovidkommande syften eller publiceras. Artikel 8 är som sagt möjlig att inskränka, och rätten att få bli lämnad ifred har i många fall prövats av Europadomstolen mot andra rättigheter och skäl, såsom förebyggande av oordning eller brott, och yttrandefriheten.⁵⁶ Avseende ett *skydd för hemmet och den enskildes korrespondens* anses skyddet för hemmet enligt artikel 8 vara en viktig aspekt av rätten till en privat sfär, vilket medför att inskränkningar i denna rätt därför kräver särskilt starka skäl. Exempel på sådana inskränkningar som har prövats och anses ligga inom denna rätt är därför sådana ingrepp som innebär att information inhämtas om enskilda genom exempelvis avlyssning, kameraövervakning eller husrannsakan. Begreppet korrespondens avser olika sätt att föra över meddelanden mellan individer och är därför förhållandevis teknikneutralt. Således omfattas bl.a. telefon, fax, radio och datorkommunikation av denna rätt.⁵⁷

Slutligen beträffande *behandling av personuppgifter och information om privata förhållanden* ställer artikel 8 krav i tre avseenden. Kraven tar huvudsakligen sikte på personregister med känsliga uppgifter såsom politisk uppfattning, sexuell läggning eller brottslighet, och inriktar sig på; (1) det berättigade i att alls registrera den ifrågavarande informationen, (2) om den enskilde ska ha en rätt att själv få ta del av dessa uppgifter, och slutligen (3) andras tillgång till de ifrågavarande uppgifterna och ett eventuellt skydd mot detta. Beträffande det andra kravet kan dock konstateras att denna rätt inte anses medföra en rätt att ta del av sekretessbelagda handlingar. Också inskränkningar av dessa tre krav är möjliga och har vid prövningar huvudsakligen rört om förutsättningarna för ett nödvändigt undantag varit uppfyllda. Ett par kända svenska fall som berört detta återges i integritetsskyddskommitténs slutbetänkande, och av dessa kan särskilt nämnas fallen Leander mot Sverige och Segerstedt-Wiberg m.fl. mot Sverige.⁵⁸

⁵⁴ SOU 2008:3, s. 86.

⁵⁵ SOU 2008:3, s. 75.

⁵⁶ SOU 2008:3, s. 76f.

⁵⁷ SOU 2008:3, s. 81f.

⁵⁸ SOU 2008:3, s. 78ff.

4 Ipred

Den 1 april 2009 trädde några väldigt uppmärksammade svenska lagändringar ikraft som i media och debatten kom att kallas ”IPRED-lagen”. Åsikterna om lagändringarnas innebörd var om inte många så åtminstone starka.⁵⁹ Tyvärr var många emellertid dåligt insatta i vad Ipred egentligen var för någonting, eller vad de (vanligen angripna) svenska lagändringarna innebar. I detta avsnitt ska därför Ipred presenteras, och de viktigaste delarna av den svenska implementeringen förklaras. Vid införandet introducerades ett helt nytt civilprocessrättsligt institut, som inte är helt okomplicerat. Följdändringar i den svenska personuppgiftslagen (PuL) gjordes också. För att i största mån undvika också framtida missförstånd måste dessa avsnitt därför med nödvändighet bli tämligen utförliga. Ipreds syfte ska kort studeras, likaså redogörs för de motiv lagstiftaren anförde till utformningen av delar av de svenska lagändringarna. Debatten kring Ipred var som högst under senhösten 2008 och våren 2009, och ett par av de vanligare argumenten mot Ipred ska därför också återges. Det har när detta skrivs gått ganska precis ett halvår sedan de svenska lagändringarna trädde ikraft, och även om det är för tidigt att utvärdera samtliga effekter av dessa ska slutligen några direkta följder och viktiga händelser som skett efter ikraftträdandet av den svenska implementeringen av Ipred skildras.

4.1 Allmänt om direktivet

Beteckningen Ipred är en förkortning av Intellectual Property Rights Enforcement Directive, vilket är det engelska namnet på ett EG-direktiv med det fullständiga svenska namnet Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter. Ipred, eller det civilrättsliga sanktionsdirektivet som det också ibland kallas, antogs med stöd av artikel 95 i EG-fördraget, och hade därför till yttersta syfte att undanröja hinder mot den fria rörligheten för varor och tjänster på EG:s inre marknad. Av direktivets ingress framgår det att ett immaterialrättsligt skydd är en grundläggande förutsättning för en framgångsrik inre marknad, främjandet av innovation och kreativitet, samt samsättning och konkurrenskraft. Därtill framhävs att det krävs ett effektivt skydd av de immateriella rättigheterna för att inte innovation, nyskapande och investeringsvilja ska dämpas, men att det finns stora skillnader mellan vilka sanktionsmöjligheter som erbjuds i de olika medlemsländerna, vilket också skadar den inre marknaden. Enligt ingressen kunde också en allt starkare koppling mellan immaterialrättsintrång och organiserad brottslighet anas, likaså bidrog den ökade internetanvändningen till att möjligheterna till immaterialrättsintrång ökade. En hög, likvärdig och enhetlig skydds nivå för immateriella rättigheter skulle således uppnås genom att harmonisera med-

⁵⁹ Se exv. Nilsson, *Artister stödjer ”IPRED-lagen”*, Aftonbladet 2008-11-13 och Olsson, *Ny fildelningslag skapar nätuppror*, Svenska Dagbladet 2008-11-12.

lemsstaternas immaterialrättsliga skyddsregler för att EG:s inre marknad ska fungera väl.⁶⁰

Den svenska implementeringen av Ipred kan och bör främst ses som en följd av Sveriges internationella förpliktelser genom sitt medlemskap i EG och EU. Direktivet skulle ha varit implementerat i samtliga medlemsstater senast den 29 april 2006, och Sverige fälldes av EG-domstolen för att inte ha gjort detta i maj 2008.⁶¹ När majoriteten av lagändringarna trädde ikraft den 1 april 2009 var den svenska implementeringen således nära tre år för sen. Även om lagstiftaren ansåg att det svenska rättsläget redan före implementeringen av Ipred uppfyllde direktivets minimikrav i flera avseenden,⁶² behandlas en stor mängd immaterialrättsliga frågor i den svenska propositionen. De ur ett juridiskt perspektiv största och mest intressanta nyheterna och förändringarna var emellertid också de som uppmärksammades och kritiserades i debatten. Det är också på dessa punkter svensk rätt tidigare företedde sina största brister i förhållande till direktivets krav. Av denna anledning bortses i detta avsnitt och resten av denna uppsats därför från de mindre, eller i förekommande fall mer allmänna, immaterialrättsliga frågor, såsom presumtion av innehav av immaterialrätter, intrångsundersökning, vitesförbud, korrigeringsåtgärder, offentliggöranden av avgöranden på intrångsgörarens bekostnad, talerätt, samt skadestånd, som också behandlas i den svenska propositionen.⁶³

De väsentliga krav som det svenska rättsläget före den 1 april 2009 således inte uppfyllde var de som ställs i direktivets artikel 8. Enligt denna bestämmelse ska de behöriga rättsliga myndigheterna i medlemsländerna få besluta att information om ursprung och distributionsnät för intrångsgörande varor och tjänster ska lämnas av intrångsgöraren och ett närmare redovisat antal andra som på ett visst sätt har befattat sig med en intrångsgörare.⁶⁴ För att inkorporera denna bestämmelse valdes en liknande metod som tidigare använts i Finland. Svensk immaterialrättslig lagstiftning är som bekant inte samlad i en central lag, och ett särskilt institut om ”informationsföreläggande” vilket ger rättighetshavare tillgång till denna typ av information vid vissa immaterialrättsintrång infördes därför i upphovsrättslagen (UrL), patentlagen, mönsterskyddslagen, firmalagen, kretsmönsterlagen och växtförädlarrättslagen.⁶⁵ För att inte omöjliggöra användandet av institutet gjordes också undantag från personuppgiftslagen i dessa lagar så att rättighetshavare skulle kunna samla in och behandla personuppgifter (företrädesvis IP-adresser vid immaterialrättsintrång via internet) om intrångsgörare utan särskilt tillstånd från datainspektionen, i den mån detta var nödvändig för att ett rättsligt anspråk skulle kunna fastställas, göras gällande, eller försvaras.⁶⁶

⁶⁰ Jfr. prop. 2008/09:67, s. 1, 71, 87f.

⁶¹ Se EG-domstolens dom C-341/07 och prop. 2008/09:67, s. 71.

⁶² Se exempelvis prop. 2008/09:67, s. 71.

⁶³ Jfr. prop. 2008/09:67, s. 2ff.

⁶⁴ Se också prop. 2008/09:67, s. 89f, 121ff.

⁶⁵ Jfr. prop. 2008/09:67, s. 127ff. Rättighetshavare syftar naturligtvis på ”fysiska eller juridiska personer som innehar immateriella rättigheter av ett kommersiellt eller ideellt värde”. Också lagstiftaren använder den mindre korrekta terminologi som används i uppsatsen.

⁶⁶ Prop. 2008/09:67, s. 172f.

4.2 Informationsföreläggandeinstitutet

Före implementeringen av Ipred fanns det inte några *generella* regler i Sverige som gav rättighetshavare en rätt till information om intrångsgörande varor och tjänsters ursprung och distributionsnät. De befintliga civilprocessrättsliga instituten edition, syn, partsförhör, vittnesförhör, och bevisupptagning till framtida säkerhet, samt det immaterialrättsliga specialinstitutet intrångsundersökning, är därtill i dessa avseenden inte av något större värde för en rättighetshavare. Begränsningar beträffande utformningen av dessa rättsmedel gör det nämligen svårt för rättighetshavare att använda dem till att identifiera okända presumtiva intrångsgörare. Vid rättighetsintrång via internet var det för en rättighetshavare därtill särskilt svårt att bevaka och försvara sina rättigheter. Exempelvis eftersom internetleverantörer m.fl. hade (och enligt huvudregeln fortfarande har) en rättsligt grundad tystnadsplikt som hindrar dem från att t.ex. frivilligt lämna ut uppgifter om abonnemang, innehåll i internettrafik eller kringuppgifter till densamma jämte 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation. Undantag från denna tystnadsplikt finns i 6 kap. 21 – 23 §§ denna lag, men gäller enbart i förhållande till de däri uppräknade myndigheterna, och kommer i princip aldrig ifråga för rättighetshavare. Det kan också klargöras att information som kan fås med hjälp av de ovan angivna civilrättsliga instituten visserligen häver denna tystnadsplikt, men att de i normalfallet likväl som sagt inte kan användas för att få information som kan användas för att identifiera en okänd intrångsgörare.⁶⁷

I den fortsatta framställningen utgås från bestämmelserna om informationsföreläggande i upphovsrättslagen, vilka hittas i 53 c – 53 f §§ UrL. Motsvarande bestämmelser återfinns i patentlagen, mönsterskyddslagen, firmalagen, kretsmönsterlagen och växtförädlarrättslagen.⁶⁸ Huvuddragen i förordningen är följande. Ett beslut om rätt till information får till att börja med endast meddelas på ansökan av en rättighetshavare, eller den som genom upplåtelse har rätt att nyttja den skyddade immaterialrätten, 53 c § 1 st. UrL. Branschorganisationer gavs således inte någon *självständig* talerätt i Sverige, och är därför enligt huvudregeln utestängda från en ansökan om ett informationsföreläggande.⁶⁹

Endast vissa rättssubjekt omfattas av skyldigheten att lämna ut information enligt direktivets artikel 8.1, och detsamma gäller enligt den svenska regleringen. För upphovsrättslagens del räknas dessa personer upp i 53 c § 2

⁶⁷ Prop. 2008/09:67, s. 121ff.

⁶⁸ Informationsföreläggandeinstitutet för dessa lagar hittas i 57 c – 57 f §§ patentlagen, 35 c – 35 f §§ mönsterskyddslagen, 18 b – 18 e §§ firmalagen, 9 c – 9 f §§ kretsmönsterlagen samt 5 a – 5 d §§ växtförädlarrättslagen.

⁶⁹ Prop. 2008/09:67, s. 95ff, 129f, 258ff. Enligt regeringen var en sådan utsträckt talerätt tillåten men fakultativ i förhållande till direktivet. Rättighetshavare har naturligtvis inte desto mindre fortfarande möjlighet att låta en branschorganisation föra dess talan i egen skap av ombud eller liknande.

st. UrL. Skyldigheten att lämna ut information omfattar därför den som har gjort eller medverkat till intrånget eller överträdelsen, i kommersiell skala har förfogat över en vara eller använt en tjänst som intrånget avser, i kommersiell skala har tillhandahållit en elektronisk kommunikationstjänst eller en annan tjänst som har använts vid intrånget eller överträdelsen, och slutligen den som har identifierats av någon av de tidigare som delaktig i tillverkningen eller distributionen av en vara eller tillhandahållandet av en tjänst som intrånget avser. Begreppet elektronisk kommunikationstjänst definieras i 1 kap. 7 § lagen om elektronisk kommunikation, och omfattar internetleverantörer och andra som tillhandahåller tjänster som huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät. Den tystnadsplikt som gäller enligt denna lag bryts dock när ett informationsföreläggande har utfärdats. Den personkrets i den svenska regleringen som ett informationsföreläggande kan riktas mot innefattar således internetleverantörer. Direktivet ställde inte något explicit krav på detta, och frågan var inte helt okontroversiell heller från lagstiftarens sida. Motiven till utformningen av den svenska regleringen återkommer dock i avsnitt 4.4 nedan. Informationsföreläggandet är vitessanktionerat, 53 c § 1 st. UrL.⁷⁰

En inte uttömmande uppräkningslista i 53 c § 3 st. UrL ger exempel på sådana uppgifter som kan omfattas av rättighetshavares rätt till information. Uppräkningen motsvarar i stort också den som görs i direktivets artikel 8.2. Ett informationsföreläggande kan därför särskilt avse; namn på och adress till producenter, distributörer, leverantörer och andra som har innehaft eller tillhandahållit intrångsgörande varor eller tjänster. Därtill kan avsedda grossister och detaljister, och uppgifter om hur mycket som har producerats, levererats, mottagits eller beställts, samt pris för intrångsgörande varor eller tjänster innefattas. Att namn på, och adress till, personer som är delaktiga i exempelvis distribution av skyddade rättigheter helt klart omfattas av rätten till information medför att en internetleverantör således kan föreläggas att lämna ut namnet på den som har haft ett visst IP-nummer vid en enskild tidpunkt om detta har använts för ett intrång (se dock nedan om sannolika skäl). Informationsföreläggandeinstitutet ålägger däremot ingen att, åtminstone i utgångsläget, spara på den information som kan bli föremål för ett informationsföreläggande. Istället ska domstolen både vid den ursprungliga prövningen, och vid ett eventuellt utdömande av förelagt vite, ta ställning till om den som yrkandet riktas mot har faktisk och rättslig möjlighet att lämna den begärda informationen.⁷¹ Av domstolens beslut ska det tydligt framgå vilken information som ska lämnas ut, samt när detta ska ske. Den som yrkandet riktas mot är också skyldig att lämna riktig och fullständig information.⁷²

Sökanden måste som sagt visa sannolika skäl för att ett intrång har begåtts, och ett beslut om informationsföreläggande får meddelas bara om informa-

⁷⁰ Prop. 2008/09:67, s. 152f, 259, 261f.

⁷¹ Det torde dock vara underförstått att den som väl fått ett föreläggande mot sig inte kan undvika att förelagt vite döms ut om informationen efter prövningen s.a.s. helt plötslig inte längre sparas.

⁷² Prop 2008/09:67, s. 157ff, 260, 262f.

tionen kan antas underlätta utredning av ett intrång eller en överträdelse, 53 c § 1 st. UrL. Naturligtvis krävs det dock inte att intrångsgöraren är identifierad. Att underlätta detta var som bekant ett av syftena med institutet. Inte heller måste några presumtiva subjektiva rekvisit visas hos intrångsgöraren. Det räcker att sannolika skäl för ett intrång i objektiv mening kan visas av sökanden för att ansökan ska kunna bifallas. Beträffande vilken typ av bevisning som skulle kunna krävas, samt att vissa former av bevisning kan vara lätta att förfalska, konstaterade lagstiftaren tämligen kort (och torrt) att svensk rätt bygger på principen om fri bevisprövning och att det är domstolarna som avgör vilken bevisning som krävs. Lagstiftaren påminde också om straffansvaren för bl.a. osann partsutsaga och osant intygande i 15 kap. 2 och 11 §§ brottsbalken. Kravet på att informationen ska underlätta utredning av ett intrång eller överträdelse innebär inte att det måste underlätta utredningen av just det intrång som informationsföreläggandet berör. Informationen måste inte heller vara avsedd för bevisning i en kommande rättegång.⁷³

Direktivets artikel 8.1 ställer krav på att ett informationsföreläggande ska meddelas om det är en berättigad och proportionell begäran. Utöver kraven i föregående stycke får ett beslut om informationsföreläggande enligt den svenska regleringen därför endast meddelas efter en proportionalitetsbedömning om skälen för åtgärden uppväger den olägenhet eller det men i övrigt som åtgärden innebär för den som drabbas av den eller något annat motstående intresse, 53 d § 1 st. UrL. Domstolen ska således i det enskilda fallet ta hänsyn till samtliga omständigheter, bl.a. den enskildes integritet. Vad gäller uppgifter som omfattas av 6 kap. 20 § lagen om elektronisk kommunikation krävs att det är fråga om intrång av en viss omfattning för att ett beslut ska kunna meddelas. Så ska i regel anses vara fallet om intrånget avser uppladdning av ett skyddat verk, eller mer omfattande nedladdning.⁷⁴

Informationsföreläggandeinstitutet är indispositivt och domstolen ska därför alltid ta ställning till om samtliga omständigheter som krävs för ett beslut om föreläggande är uppfyllda. Ett yrkande om rätt till information kan göras oberoende av om det pågår en rättegång om rättighetsintrång eller inte, och skyldighet att lämna ut information föreligger först när en domstol har prövat och bifallit ansökan.⁷⁵ Fram tills denna tidpunkt fortsätter således befintliga tystnadsplikter och liknande att gälla. Uppgifter som har erhållits genom ett informationsföreläggande får dock inte användas i strid mot bestämmelserna i personuppgiftslagen, se också avsnitt 4.3 nedan. Slutligen ska den som lämnat ut information som omfattas av 6 kap. 20 § lagen om elektronisk kommunikation underrätta den som uppgifterna gäller skriftligen tidigast en månad, och senast tre månader, efter detta skett, 53 f § 2 st. UrL. Således ska en internetleverantör som lämnat ut uppgifter om vilken abonnent som använt ett visst IP-nummer vid en viss tidpunkt underrätta sin abonnent om detta inom denna tidsfrist.⁷⁶

⁷³ Prop. 2008/09:67, s. 149ff, 258ff.

⁷⁴ Prop. 2008/09:67, s. 160ff, 264f.

⁷⁵ Prop. 2008/09:67, s. 145ff, 259.

⁷⁶ Prop. 2008/09:67, s. 169, 268f.

4.3 Trafikdata och personuppgiftsskydd

Som sagt gjordes också vissa ändringar i den svenska personuppgiftslagen vid genomförandet av Ipred för att informationsföreläggandeinstitutet⁷⁷ skulle gå att använda i praktiken. Tillämpningsområdet för personuppgiftslagen är väldigt brett, och omfattar all helt eller delvis automatiserad behandling av personuppgifter, och all annan behandling om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier, 5 § PuL. Personuppgifter är enligt PuL all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, 3 § PuL. All hantering av personuppgifter som omfattas av PuL:s tillämpningsområde omfattas också av lagens i många fall långtgående krav. Således får behandlingen bl.a. inte omfatta fler personuppgifter än vad som är nödvändigt, de får inte användas på ett sätt som är oförenligt med det syfte som de samlades in, och de får inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till behandlingens ändamål, 9 § PuL. Lagens tillsyn övervakas av datainspektionen, som har vittgående befogenheter att med påpekanden och viten se till att lagen efterföljs, jfr. 43 – 47 § PuL. Personuppgiftslagen innehåller också bestämmelser om skadestånd och straff i 48 och 49 §§.⁷⁸

Således omfattas de flesta tänkbara tillvägagångssätt rättighetshavare som i större omfattning söker identifiera intrångsgörare kan använda av personuppgiftslagens krav och bestämmelser. Dessutom omfattas samtliga uppgifter som kan bli föremål för ett informationsföreläggande av personuppgiftslagen, och samma krav ställs således på behandlingen av dessa uppgifter som rättighetshavare (och alla andra) också i andra sammanhang har att rätta sig efter. En påminnelse om att missbruk av uppgifter som fås genom ett föreläggande är förbjudet infördes därför också i 53 d § 3 st. UrL.⁷⁹ Personuppgiftslagen innehåller emellertid också ett fåtal bestämmelser om särskilt känsliga personuppgifter som ställer ännu strängare krav på, och i vissa fall förbjuder, vissa rättssubjekts behandling av personuppgifter. De flesta immaterialrättsliga intrång är straffsanktionerade, och enligt 21 § 1 st. PuL är det förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelse som innefattar brott. Datainspektionen var därför för ett par år sedan nära att ingripa mot ett par flagranta överträdelse av 21 § PuL begångna av företrädare för rättighetshavare, men meddelade i slutändan dispens för vissa sådana organisationer att i större omfattning behandla vissa personuppgifter såsom IP-adresser varifrån främst upphovsrättsliga rättighetsintrång via internet begåtts.⁸⁰

⁷⁷ Vilket är ett hemskt, hemskt ord. Eftersom det är lagstiftaren som har myntat det bör inte författaren lastas för att det används i uppsatsen (ett minimalt antal gånger).

⁷⁸ Se också prop. 1997/98:44, s. 117ff och prop. 2008/09:67, s. 167f.

⁷⁹ Se också prop. 2008/09:67, s. 168f.

⁸⁰ Se också prop. 2008/09:67, s. 172f.

En sådan dispens kan i samband med implementeringen av Ipred sägas ha permanentats genom att ett generellt undantag från 21 § PuL infördes i 53 g § UrL,⁸¹ för att möjligheterna att använda sig av informationsföreläggandeinstitutet inte helt skulle stoppas. Således får personuppgifter om lagöverträdelse som innefattar brott behandlas om detta är nödvändigt för att ett rättsligt anspråk ska kunna fastställas, göras gällande eller försvaras. Lagstiftaren var dock väldigt noga med att understryka att de övriga bestämmelserna i personuppgiftslagen (som sagt) fortfarande gäller och måste uppfyllas för att behandlingen inte ska ske på ett integritetskränkande sätt, samt att datainspektionen också fortsättningsvis utövar tillsyn. Undantaget ger därför inte heller någon rätt att exempelvis upprätta ett systematiskt register över internetanvändare som misstänks syssla med olaglig fildelning.⁸²

4.4 Motiven till implementeringen

I allmänhet ligger den svenska implementeringen av Ipred tämligen nära direktivets mening och innebörd. Beträffande informationsföreläggandeinstitutet har som framgått i avsnitt 4.2 ovan utformningen också till stor del styrts av direktivet. När anledningen till den valda utformningen av lagstiftningen rörande rätten till information återgivits i propositionen har därför i de flesta fall enbart rent praktiska frågor berörts. Någon egentlig diskussion eller motivering till vald utformning, utöver att svensk rätt ska uppfylla de krav som ställs i direktivet, har därför i de flesta fall inte förts eller återgetts – av den enkla anledningen att direktivets krav i många fall ansetts vara ganska klara, samt att den svenska regleringen inte avsetts ställa mer långtgående krav. Det finns dock undantag. Direktivet lämnar i vissa detaljer tämligen fritt åt medlemsstaterna att närmare bestämma omfattningen av den nationella regleringen.

De frågor som är särskilt viktiga ur ett integritetsperspektiv, vilka också råkar sammanfalla med de delar av den svenska regleringen som allra hårdast har kritiserats, diskuteras därför mer utförligt i den svenska propositionen. I dessa avseenden skiljer sig också den faktiska utsträckningen av implementeringen åt i de olika medlemsstaterna. Därför ska motiven till (delar av) utsträckningen av den personkrets som omfattas av den svenska skyldigheten att lämna information nu studeras närmare. Det kan också inledningsvis påpekas att mest intressant ur integritetshänsyn vad gäller informationsföreläggandeinstitutet torde främst vara vem som har rätt till information, vem som omfattas av skyldigheten att lämna ut information, samt vilken typ av information som omfattas. I den första och sista av dessa bägge frågor ställer Ipred tämligen tydliga krav.⁸³ Med ett medlemskap i EG/EU bör en kritik mot svaret på dessa frågor således i första hand inte föras gentemot den svenska lagstiftaren. Detta har dock inte heller skett i de flesta fall.

⁸¹ Identiska bestämmelser för de övriga immaterialrättsliga lagarna återfinns i 57 g § patentlagen, 35 g § mönsterskyddslagen, 18 f § firmalagen, 9 g § kretsmönsterlagen och 5 e § växtförädlarrättslagen.

⁸² Prop. 2008/09:67, s. 173, 269.

⁸³ Jfr. prop. 2008/09:67, s. 129f & 157ff.

De motiv som angavs för undantagen till personuppgiftsskyddet återgavs kortfattat i avsnitt 4.3 ovan.

En relativt detaljerad uppräkningslista av vem som ska lämna information om ursprung och distributionsnät för intrångsgörande varor och tjänster görs som sagt i artikel 8.1 Ipred. Bortsett från att de svenska medverkans-, samt försöks- och förberedelsebestämmelserna möjligen inkluderar en marginellt bredare personkrets än den som avses i denna uppräkningslista orsakade så långt därför inte heller artikel 8.1 lagstiftaren några större problem. Direktivets bestämmelser fördes också i denna del således mer eller mindre rakt över till svensk rätt.⁸⁴ Utgångspunkten i Ipred är att också rättighetsintrång som sker via internet omfattas av rätten till information. I artikel 8.3(e) påpekas det dock att skyldigheten att lämna information inte ska påverka tillämpningen av andra lagbestämmelser som reglerar sekretesskydd för informationskällor eller behandling av personuppgifter. Vilket redan har berörts på ett flertal ställen ovan reglerar och begränsar flera bestämmelser i både personuppgiftslagen och lagen om elektronisk kommunikation sådan information som kan bli föremål för en rätt till information, och i liknande situationer som när denna rätt kan aktualiseras. Dessa bägge lagar bygger därtill egentligen på två andra EG-direktiv,⁸⁵ och det är också dessa direktiv som artikel 8.1(e) särskilt åsyftar.⁸⁶

Vilka regler går då först? Lagstiftaren konstaterade kort att kommissionen och samtliga medlemsstater vid utarbetandet av Ipred var överens om att rätten till information inte begränsades av dessa andra direktiv och att exempelvis internetleverantörer ska inkluderas i den personkrets som omfattas av skyldigheten att lämna ut information.⁸⁷ Frågan hamnade på omvägar dock också hos EGD, som i mål C-275/06 uttalade att Ipred *inte* ålägger medlemsstaterna en *skyldighet* att införa bestämmelser innebärande att rättighetshavare kan begära ut uppgifter från internetleverantörer om vem som har haft en viss IP-adress vilken har använts vid ett rättighetsintrång. Medlemsstaterna är dock skyldiga att tillhandahålla ett effektivt egendomsskydd, vartill immaterialrätterna räknas. Egendomsskyddet måste också vägas mot skyddet av privatliv, och i slutändan är det enligt EGD upp till medlemsstaterna att efter eget skön fritt söka uppnå en balans mellan egendomsskyddet och skyddet för privatliv.⁸⁸ Således var det upp till regeringen att avgöra om internetleverantörer skulle inkluderas i den personkrets som kunde vara skyldiga att lämna information.

Hur utslaget föll har redan berörts. Lagstiftaren konstaterade att det sker en omfattande piratkopiering på internet i Sverige, och att denna kan motverkas på en rad olika sätt. För detta har branschen ett stort ansvar, men också lag-

⁸⁴ Jfr. prop. 2008/09:67, s. 130ff.

⁸⁵ De för den personliga integriteten mycket viktiga lagarna bygger beträffande personuppgiftslagen således på dir. 94/46/EG, och beträffande lagen om elektronisk kommunikation på dir. 2002/58/EG.

⁸⁶ Prop. 2008/09:67, s. 134f.

⁸⁷ Prop. 2008/09:67, s. 135.

⁸⁸ Se särskilt p. 70 i domstolen dom C-275/06, och prop. 2008/09:67, s. 136f.

stiftaren har ett ansvar, och måste tillhandahålla tydliga spelregler med effektiva, rättssäkra och balanserade möjligheter att ingripa mot den olagliga piratkopieringen. Vidare sades att det för rättighetshavare är angeläget att kunna härleda vem som begår rättighetsintrång för att kunna kontakta denna person och kräva att han eller hon ser till att intrånget upphör, vilket ofta borde vara tillräckligt för att intrånget ska upphöra. Därtill saknades tidigare ofta möjligheter att använda sig av andra civilprocessuella rättsmedel såsom edition och intrångsundersökning för att säkra bevisning, och i förlängningen föra en civilrättslig talan och kräva skadestånd eftersom denna kunskap inte var möjlig att nå. De enda utvägarna i dessa fall för de flesta rättighetshavare var tidigare att be internetleverantörerna att kontakta sina kunder eller att polisanmäla. Regeringen ansåg emellertid det inte vara rimligt att endast polis eller åklagare kunde ingripa mot rättighetsintrång på internet. Det var istället i många fall mer lämpligt om rättighetshavare gavs en utökad möjlighet att göra detta själva. Ett komplement till de straffrättsliga åtgärderna skulle skapas, möjligheterna att ingripa mot rättighetsintrång via internet skulle öka, och detta skulle på så sätt samtidigt bli en faktor för att främja den fortsatta utvecklingen av konsumentvänliga tjänster på internet enligt lagstiftaren.⁸⁹

Eventuell problematik kring anonymisering och öppna trådlösa nätverk⁹⁰ avfärdades däremot. Problematiken ansågs vara densamma oavsett om ett straffrättsligt eller ett civilrättsligt perspektiv antogs, och hade därför inte någon omedelbar betydelse för om utgångspunkten borde vara att endast polis och åklagare ska ingripa mot alla rättighetsintrång på internet, eller om också rättighetshavare skulle ges utökade befogenheter. Därtill anfördes att avtalsvillkoren för internetanslutning ofta innehåller bestämmelser om att denna enbart får användas för privat bruk samt att abonnenten i vissa fall kan hållas ansvarig gentemot internetleverantören för andras användning av uppkopplingen. Av denna anledning, och för att undvika att uppkopplingen används av andra i brottsligt syfte, var det enligt lagstiftaren därför i personens eget intresse att skydda sitt hemnätverk från obehörig användning. Man hänvisade också till att det på Post- och telestyrelsens hemsida finns information om hur man gör detta.⁹¹

Att internetleverantörer skulle omfattas av den personkrets ett informationsföreläggande kunde riktas mot ogillades enbart av ett fåtal remissinstanser, där särskilt Juridiska fakultetsstyrelsen vid Lunds universitet, Post- och Telestyrelsen, Tullverket och Datainspektionen kan nämnas som några som avstyrkte att informationsskyldigheten skulle utsträckas så långt eller ställde sig tveksamma till förslaget. Datainspektionen ställde sig därtill frågande till om utsträckningen var förenlig med EG:s regler om dataskydd och artikel 8 EKMR. Beträffande artikel 8 EKMR konstaterade regeringen att det visser-

⁸⁹ Prop. 2008/09:67, s. 138ff.

⁹⁰ Med detta avses trådlösa hemnätverk som är inställda på sådant sätt att vem som helst som är inom täckningsområdet kan ansluta till internet genom abonnentens anslutning utan lösenord eller inloggningsuppgifter.

⁹¹ Prop. 2008/09:67, s. 140f.

ligen var fråga om en inskränkning av rätten till privatliv, men att förutsättningarna för ett undantag i enlighet med artikel 8.2 också var för handen.⁹²

Lagstiftaren gjorde avslutningsvis en proportionalitetsbedömning. Rättighetshavare hade enligt de skäl som återgetts ovan ett starkt intresse att få tillgång till personuppgifter kring abonnemangsinnehavare av en IP-adress, och dessa intressen skulle vägas mot det integritetsintrång som blev resultatet av att abonnentens identitet röjs. Beträffande integritetsintrånget kunde detta anses vara begränsat, eftersom den information som åtkoms genom ett informationsföreläggande är betydligt mer begränsad än den som kan åtkommas genom andra civilprocessuella institut. Av tekniska orsaker, och eftersom de flesta har dynamiska IP-adresser vilka ändras över tiden, var det enligt lagstiftaren inte heller möjligt att använda uppgifter kring IP-nummer för att mer allmänt kartlägga vad enskilda personer gör på internet. Det anfördes också att en mer allmän kartläggning enligt PuL inte får göras utan den enskildes samtycke. Behovet av ytterligare åtgärder mot intrång via internet var samtidigt starkt. Därför konstaterades att intresset att få ut denna information väger tyngre än det men som abonnenten drabbas av.⁹³

Slutligen uttalade regeringen i propositionen att de särskilt ska följa och utvärdera hur många ärenden de nya bestämmelserna ger upphov till och hur den överkomna informationen används. Framförallt ska följas i vilken utsträckning informationen används för att skicka ut varningsbrev och för att inleda en domstolsprocess, samt om bestämmelserna används för att vidta åtgärder mot intrång i stor omfattning.⁹⁴ Redan under sommaren 2009 tillsatte regeringen en särskild utredare för att titta på just dessa frågor.⁹⁵

4.5 Kritik mot implementeringen

Under senhösten 2008 och våren 2009 fördes en relativt långlivad integritetsdebatt i Sverige. Den del av debatten som främst kritiserade genomförandet av Ipred riktade sig i första hand mot den omfattning informationsföreläggandeinstitutet kommit att få, och särskilt sakförhållandet att internetleverantörer kom att inkluderas i den personkrets som kan bli föremål för ett utlämnande av information, samt de integritetsintrång som därmed i förlängningen blir resultatet för den enskilde. Det är svårt att överblicka ett helt debattområde, och integritetsdebatten har dessutom till stor del förts utanför de s.a.s. mer traditionella medierna. Avsikten med detta avsnitt är enbart att ge några exempel på argument som förts gentemot den omfattning den svenska rätten till information kommit att få. Detta är varken någon översikt eller uttömmande studie över hur debatten har förts, eller en sammanfattning av densamma. Inledningsvis kan också konstateras att det i vissa fall kan misstänkas att kritiken och oppositionen mot Ipred varit felriktad. I dessa

⁹² Prop. 2008/09:67, s. 135f, 141ff, 173. Beträffande artikel 8 EKMR, se också avsnitt 3.4.

⁹³ Prop. 2008/09:67, s. 141f.

⁹⁴ Prop. 2008/09:67, s. 174.

⁹⁵ TT, *Ipredlagen utvärderas*, Dagens Nyheter 2009-07-23.

fall ligger missnöjet förmodligen mindre i den omfattning rätten till information kommit att få, än i utformningen av den nuvarande upphovsrätten. Denna fråga har avsiktligt exkluderats ur denna uppsats.

I de fall kritiken har särskilt specificerat på vilket sätt den svenska implementeringen är integritetskränkande, och inte bara mer allmänt uttryckt en sådan ståndpunkt, har denna främst riktat sig mot att rättighetshavare ska få tillgång till information om abonnemangsinnehavare som står bakom en IP-adress. Den nya regleringen ansågs av vissa således medföra att en privatisering av delar av brottsbekämpningen skedde eftersom rättighetshavare och lobbyorganisationer övertog polisiära uppgifter, och regeringen vek ned sig för deras intressen.⁹⁶ Farhågor restes också kring risken för en form av ”legaliserad utpressning”. Resultatet i andra länder där rättighetshavare har tillgång till sådan information skulle vara att rättighetshavar- och branschorganisationer skickat brev med hot om stora skadeståndskrav till privatpersoner, vari ett förlikningsförslag om en lägre summa föreslogs varvid domstolsprocesser med redan nämnda höga skadeståndsbelopp och ännu högre rättegångskostnader undveks. Att redan andras tillgång till, och behandling av, personuppgifter är integritetskränkande samt risken för läckor har också framförts. Därtill har också framhållits rättssäkerhetsaspekter såsom att en abonnemangsinnehavares innehav av en IP-adress inte är detsamma som att denna person har stått för rättighetsintrånget.⁹⁷

Som nämndes i inledningen till detta kapitel fanns det också allt för många missförstånd kring vad innebörden i den svenska implementeringen av Ipred var. Ett väldigt (ned-)slående exempel på detta var tidningen Datormagazins presentation av implementeringen av Ipred. Bl.a. sades att lagstiftningen skulle innebära att abonnenten blir direkt ansvarig för olagliga åtgärder som skett från adressen, samt att samma regler som gäller för P-böter nu också skulle gälla för fildelning.⁹⁸ Det kan tilläggas att Datormagazin beskriver sig som Sveriges största tidning för avancerade datoranvändare, professionella webbproducenter och IT-utvecklare,⁹⁹ och har en upplaga om 21 300.¹⁰⁰ En annan missuppfattning har varit att multinationella skiv- och filmbolagsjättar med Ipred skulle ges polisiära befogenheter och möjligheter att göra husrannsakan hos misstänkta.¹⁰¹ Att denna okunskap också verkar ha funnits hos vissa riksdagsledamöter är uppseendeväckande.¹⁰² Slutligen går det givetvis att konstruera tankeexempel där reglerna skulle kunna användas i helt andra syften av exempelvis religiösa sekter eller politiska ex-

⁹⁶ Hammarqvist, *Alliansens svek mot den personliga integriteten*, Norra Skåne, 2009-02-24, *Mesta motståndets lag*, Huvudledare Sydsvenskan 2009-03-18.

⁹⁷ Gustafsson, ”*Fildelarlagen farligare än FRA-lagen*”, Dagens Nyheter 2008-11-29, Hammarqvist, *Alliansens svek mot den personliga integriteten*, Norra Skåne, 2009-02-24.

⁹⁸ Brinkhäll, *Så enkelt lurar du FRA*, Datormagazin nummer 3 2009. Rättighetshavare skulle också åtala intrångsgörare. I dessa delar innehåller artikeln så många faktafel att jag inte vet var jag ska börja.

⁹⁹ <http://www.hjemmetmortensen.se/produkter/datormagazin/> (2009-12-18).

¹⁰⁰ <http://www.ts.se/Mediefakta/Index.aspx?mc=004306> (2009-12-18).

¹⁰¹ Jfr. *Mesta motståndets lag*, Huvudledare Sydsvenskan 2009-03-18.

¹⁰² Jfr. Olsson, *Klart nej till ny fildelningslag*, Svenska Dagbladet 2009-03-17.

tremgrupper,¹⁰³ men dessa fall kommer troligtvis minst sagt att tillhöra undantagen.

4.6 Händelser efter implementeringen

Den svenska implementeringen av Ipred trädde till övervägande del ikraft den 1 april 2009. Det är som sagt alldeles för tidigt att utvärdera denna lagstiftning. I detta avslutande avsnitt ska dock ett antal viktiga händelser med direkt anknytning till lagändringarna samt den tillhörande debatten återges. I bakvattnet till debatten och den omfattande kritik som den svenska implementeringen av Ipred fick, gick veckorna efter ikraftträdandet en större och två mindre internetleverantörer ut med att de inte längre skulle spara de uppgifter som krävdes för att en rättighetshavare med hjälp av ett IP-nummer skulle kunna begära ut vem som var abonnemangsinnehavare vid en enskild tidpunkt.¹⁰⁴ Som berördes i avsnitt 4.2 ovan åläggs ingen i utgångsläget att spara på den information som kan bli föremål för ett informationsföreläggande. En av de mindre operatörerna erbjöd (och erbjuder fortfarande kan tilläggas) utöver detta samtliga sina abonnenter en gratis anonymiseringstjänst, där all abonnentens internettrafik leds ut på internet genom en VPN-tunnel mellan abonnenten och en proxyserver.¹⁰⁵ Detta omöjliggör i praktiken spårning av trafik till ett enskilt IP-nummer – och i förlängningen till en enskild abonnent eller användare.¹⁰⁶ I dagsläget marknadsför ett ytterligare antal mindre internetleverantörer sina abonnemang som integritetsmärkta.¹⁰⁷ Huruvida detta förfarande kommer att kunna fortgå kommer delvis att beröras i avsnitt 6.5 nedan. Inga formella indikationer på förändring av det nuvarande rättsläget verkar åtminstone finnas inom det strikt immaterialrättsliga området. Det kan slutligen också tilläggas att beträffande den största av de ursprungliga operatörerna, Tele 2, verkar ställningstagandet numera ha tagits tillbaka av marknadsföringen på deras hemsida att döma.¹⁰⁸

¹⁰³ Gustafsson, "Fildelarlagen farligare än FRA-lagen", Dagens Nyheter 2008-11-30.

¹⁰⁴ Nilsson, *Tele 2 raderar Ipreduppgifter*, Svenska Dagbladet 2009-04-28 och Svantesson, *Tele 2 går runt Ipredlagen*, Dagens Nyheter 2009-04-27.

¹⁰⁵ Det finns ingen anledning till att göra någon större djupdykning i dessa tekniska begrepp. Kortfattat kan tekniken sägas gå ut på att man upprättar en ej avlyssningsbar (krypterad) anslutning mellan abonnenten och en server någon annan stans på internet (både geografiskt och med en annan IP-adress). Därefter leds *all* abonnentens trafik genom denna anslutning till servern innan den s.a.s. leds ut på "resten" av internet. I de allra flesta fall leds samtidigt många andra användares trafik samtidigt ut via samma server. Eftersom anslutningen mellan abonnenten och servern inte går att avlyssna (åtminstone utan ansträngning), och abonnentens trafik när den leds ut på internet via den avlägsna servern är uppblandad med många andra användares, blir det i praktiken omöjligt att härleda enskild trafik till en bakomliggande användare utan tillgång till den använda servern.

¹⁰⁶ TT, *Bredbandsoperatör döljer fildelande*, Sydsvenskan 2009-05-14.

¹⁰⁷ Se anslutna operatörer på sidan iNTeGriTY – integritetsmärkt bredband (<http://integrity.st/2009-10-14>).

¹⁰⁸ Utan att skriva läsaren på näsan allt för mycket kan kanske nämnas att Tele 2 är en del i Stenbeck-/Kinneviksfären, vari bl.a. också MTG ingår.

Timmarna och dagarna efter ikraftträdandet av den svenska implementeringen rapporterades det från ett flertal håll om att internettrafiken i Sverige minskat med så mycket som 40 %. Som också delvis framgick i dessa artiklar borde dock denna statistik kanske tas med en (rejäl) nypa salt.¹⁰⁹ Hur det än var med denna sak verkade trafiken emellertid hämta sig en kort tid därefter.¹¹⁰ Naturligtvis är det över huvud taget dock tveksamt huruvida en ökad efterlevnad av främst upphovsrättslig lagstiftning kan studeras enbart genom att titta på indirekt statistik över internettrafik, och en komplett utvärdering av lagen är som sagt för tidig att göra. En annan enligt de flesta mer eller mindre direkt följd av integritetsdebatten var att Piratpartiet tog sig in i Europaparlamentet genom Europaparlamentsvalet den 7 juni 2009. Partiet fick genom sina 7 % av rösterna ett mandat, och kommer att få ytterligare ett mandat i parlamentet så fort Lissabonfördraget träder ikraft.¹¹¹

Det första yrkandet om ett föreläggande enligt 53 c § UrL lämnades slutligen in till Solna tingsrätt under natten den 1 april 2009. Detta ärende, vari yrkandet bifölls av tingsrätten, överklagades sedermera till Svea hovrätt, som meddelade den första överrättsprövningen av en begäran om informationsföreläggande den 13 oktober 2009. I ärendet prövades dels om datalagringsdirektivet utgör hinder mot att abonnentuppgifter avseende en viss IP-adress får lämnas till annan än myndighet i enlighet med 53 c § UrL,¹¹² och dels om sökanden visat sannolika skäl för att ett upphovsrättsligt förfogande genom överföring av verk till allmänheten hade skett. Hovrätten konstaterade först att det inte fanns någon normkonflikt mellan datalagringsdirektivet och 53 c § UrL. Beträffande sannolika skäl rörde ärendet en FTP-server där 27 upphovsrättsligt skyddade ljudböcker fanns att ladda ned för personer med rätt inloggningsuppgifter. Det fanns dock ingen utredning kring vad som krävdes för att få tillgång till dessa inloggningsuppgifter, eller inom vilka kretsar de hade spritts. Det fanns i ärendet inte heller någon utredning kring hur branschorganisationen Antipiratbyrån hade fått tillgång till inloggningsuppgifterna,¹¹³ eller om någon annan än de kunnat ladda ned från servern. Det gick av dessa skäl därför enligt hovrätten inte heller att dra några slutsatser om vad som krävdes för att få tillgång till användaruppgifterna eller i vilken omfattning de hade spridits. Hovrätten ansåg på grund därav att omständigheterna i ärendet också var förenliga med ett antagande att verken överförts endast till en sluten krets. Sökanden hade därmed inte visat sannolika skäl för att ett upphovsrättsintrång förelåg, och hovrätten upphävde därför tingsrättens beslut. Det bör slutligen också tilläggas att två av rättsens ledamöter var skiljaktiga i denna del, och att ordförandens röst var utslagsgivande i ärendet.¹¹⁴

¹⁰⁹ Goldberg, *Internettrafiken dyker*, IDG.se 2009-04-01, Lewan, *Internettrafiken halverades igår*, Ny Teknik 2009-04-02, Stiernstedt, *Internettrafiken minskade*, Dagens Nyheter 2009-04-02.

¹¹⁰ TT, *Full fart på fildelningen igen*, Dagens Nyheter 2009-06-18.

¹¹¹ Brandel, *Piratpartiet EU-valets stora segrare*, Svenska Dagbladet 2009-06-08.

¹¹² Datalagringsdirektivet återkommer i kapitel 6 nedan.

¹¹³ I många sammanhang har erinrats om tillämpningsområdet för 4 kap. 9 c § brottsbalken. Se exv. Rickardsson, *”Antipiratbyrån kan ha begått dataintrång”*, Svenska Dagbladet 2009-04-05.

¹¹⁴ Se Svea hovrätts beslut ÖÄ 6091-09.

5 Telekompaketet

Sedan hösten 2007 har det pågått ett intensivt, och som det har framställts också infekterat, arbete inom EU för att förnya det mycket omfattande gemenskapsrättsliga regelverket för elektroniska kommunikationer. Regelverket består idag av fem direktiv och fyra andra dokument, och samlingsnamnet för dessa är vanligen Telekompaketet, med hänvisning till det område som rättsakterna reglerar.¹¹⁵ Olyckligtvis har detta också varit den vanligast förekommande beteckningen på de ändringar av detta regelverk som just har antagits.¹¹⁶ Den kommande regleringen har åtminstone enligt vissa förslag haft förutsättningar att få en stor betydelse för internet och framtida elektronisk kommunikation inom den Europeiska unionen, och är därför i allra högsta grad aktuell att studera inom ramen för denna uppsats.

Inledningsvis redogörs i detta kapitel kort för vad det befintliga regelverket reglerar i dagsläget. Detta område är som sagt mycket omfattande, och tämligen komplicerat både ur en rent juridisk synvinkel, som ur en teknisk sådan. Eftersom huvuddelen av detta regelverk därtill inte direkt tangerar de frågor som berörs i denna uppsats i övrigt samt att regleringen också är hjälpligt okontroversiell, har framställningen i denna del gjorts översiktlig. Telekompaketet har under våren 2009 varit tämligen uppmärksammat i de traditionella medierna, och det utdragna arbetet har på nytt märkts under hösten 2009. Det är företrädesvis två detaljer i Telekompaketet som både orsakat striden mellan Europaparlamentet och rådet och samtidigt varit den del i regleringen som uppmärksammas och kritiserats i den omkringgårdande debatten. I de efterkommande avsnitten i detta kapitel ska därför de föreslagna ändringarna, och särskilt tvisteämnet mellan Europaparlamentet och rådet, återges samt viss möjlig bakgrundsfakta till detsamma. De viktigaste turerna i det utdragna antagningsförfarandet ska också skildras, samt något nämnas om den omkringgårdande debatten och kritiken mot den föreslagna nya regleringen vilken har kritiserats bl.a. ur integritetssynpunkt.

5.1 Huvuddragen i nuvarande reglering

Det nuvarande EG-rättsliga ramverket för elektroniska kommunikationer bygger som sagt på fem direktiv, och fyra andra rättsakter (som här kan bortses från). Dessa fem direktiv, vilka vanligen kallas för ramdirektivet, auktorisationsdirektivet, tillträdesdirektivet, direktivet om samhällsomfattande tjänster och användares rättigheter, samt direktivet om integritet och elektronisk kommunikation,¹¹⁷ är i svensk rätt huvudsakligen implemente-

¹¹⁵ Jfr. regeringskansliet faktapromemoria 2007/08:FPM45.

¹¹⁶ I denna uppsats har dock tydliggjorts vilken av regleringarna som avses; den nuvarande eller den kommande.

¹¹⁷ De fullständiga beteckningarna på dessa direktiv är, i samma ordning som de återges ovan, Europaparlamentets och rådets direktiv 2002/21/EG om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/20/EG om

rade genom den redan tidigare berörda lagen om elektronisk kommunikation, samt genom ett par bestämmelser i lagen (1998:31) om standarder för sändning av radio- och TV-signaler. Det nuvarande ramverket antogs 2001, men föregicks av ett snårigt tidigare regelverk för telekommunikationer som under 1990-talet syftade till att öppna de dåvarande medlemsländernas nationella telemarknader för konkurrens.¹¹⁸

Också det nuvarande regelverket syftar med denna bakgrund till att i första hand uppnå ökad konkurrens och harmonisering på området för elektronisk kommunikation, för att bl.a. tillförsäkra slutkunderna på de nationella marknaderna ett ökat utbud, lägre priser och bättre kvalitet. För att uppnå detta syfte tillhandahåller regelverket en mängd olika instrument och regleringar. Till att börja med bygger den nuvarande regleringen på att nationella tillsynsmyndigheter utför analyser av hur de olika marknaderna fungerar, samt utövar tillsyn för att förverkliga detta huvudsyfte. För Sveriges del utövar Post- och telestyrelsen tillsyn, och kan för enskilda dominerande aktörer med ett betydande inflytande på en enskild marknad inom telekommunikationssektorn införa särskilda skyldigheter för denna aktör.¹¹⁹

Andra viktiga frågor som regleras i regelverket är bl.a. förvaltning och användning av radiofrekvenser och nummer, regler kring förenkling av inträde på marknader för elektronisk kommunikation och elektroniska tjänster för nya aktörer – varvid bl.a. särskild tillståndsplikt för sådan verksamhet är förbjuden, frågor kring samtrafik mellan och tillträde till olika leverantörers kommunikationsnät och tillhörande faciliteter, grundläggande säkerhets- och driftstillförlitlighetskrav för ifrågakvarande former av kommunikationsnät, avgiftsfri koppling till ett gemensamt europeiskt larmnummer (112), vilken grundinformation konsumenter har rätt till i avtalsförhållanden med tjänsteleverantörer, obligatoriska radio- och TV-sändningar vilka leverantörer måste tillhandahålla konsumenter (s.k. must carry-utbud), och säkerställande av konfidentialitet vid kommunikation bl.a. genom krav på förbud mot avlyssningsåtgärder, upptagning med tekniska hjälpmedel, lagring eller andra metoder som innebär att kommunikation och därmed förbundna trafikuppgifter fångas upp eller övervakas utan samtycke och/eller lagligt stöd.¹²⁰

Med några få undantag regleras således *inte* frågor kring restriktioner i tillgång till, eller frågor om innehåll och/eller utbud i, den elektroniska kommunikationen eller tjänsterna i det nuvarande regelverket. Inte heller regle-

auktorisation för elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/19/EG om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande utrustning, direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster samt direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

¹¹⁸ Regeringskansliet faktapromemoria 2007/08:FPM45, jfr. prop. 2002/03:110, s. 73ff.

Sverige är långt ifrån ensamt om att ha haft reella (eller faktiska) monopol på dessa marknader.

¹¹⁹ Regeringskansliet faktapromemoria 2007/08:FPM45.

¹²⁰ Se också prop. 2002/03:110, s. 64ff, där den nuvarande regleringen återges mer utförligt.

ras frågor som en (medborgerlig) rätt till fullständig eller ocensurerad internetillgång, rättssäkerhetsfrågor såsom en rätt till rättslig prövning i fråga om tillgång, övergripande straff- eller civilprocessrättsliga aspekter eller immaterial- och upphovsrättsliga problem såsom exempelvis fildelning i det nu gällande regelverket i endera riktningen.

5.2 Huvudsakligt innehåll i förslaget

Av regelverket framgår att reglerna regelbundet ska ses över. Reformförslagen bygger av denna anledning på en översyn kommissionen utförde under 2006 och 2007. Kommissionen lade fram två förslag på ändringsdirektiv, där det ena vilket kallades ”bättre reglering” innehöll ändringar i ramdirektivet, tillträdesdirektivet och auktorisationsdirektivet, och det andra vilket kallades ”medborgarnas rättigheter” innehöll ändringar i direktivet om samhällsomfattande tjänster och användares rättigheter, samt direktivet om integritet och elektronisk kommunikation.¹²¹ Vilket också framgår av regeringens faktapromemoria om Telekompaketet, leder översynen och kommissionens förslag i utgångsläget inte till någon genomgripande förändring eller modifikation av de grundläggande förutsättningarna eller målen i det gällande regelverket. Förslagen avsågs utgöra en uppdatering och modernisering av den nuvarande regleringen med hänsyn till den utveckling som har skett sedan 2001 på området.¹²²

Också den nya regleringen syftar till en ökad konkurrens och harmonisering inom den elektroniska kommunikationssektorn. Kommissionen och de nationella regleringsmyndigheterna avses koncentrera sig på de mest betydande hindren för en fungerande konkurrens, och de nationella myndigheterna ska få en förstärkt roll i förhållande till den de har i dagsläget. De nationella regleringsmyndigheterna som bl.a. utövar tillsyn över den nationella marknaden ska kunna ålägga en enskild dominerande aktör med ett betydande inflytande på en enskild marknad att sälja tillträde till en nödvändig del av den egna infrastrukturen till sina konkurrenter, för att uppnå en tillfredsställande konkurrens. Man avsåg också att ytterligare harmonisera tillämpningen av dessa delar av regleringen mellan de olika medlemsstaterna med det nya regelverket.¹²³

Allra störst utrymme i kommissionens förslag till ny reglering har dock tillgången till, och användningen av, det begränsade radiofrekvensspektrat. Den tidigare regleringen har lett till en fragmenterad användning, och tjänste- och teknikneutralitet införs med förslaget som huvudregel för frekvens-

¹²¹ De ursprungliga direktivförslagen från kommissionen har beteckningarna KOM(2007) 697 respektive KOM(2007) 698. Utöver de bägge förslagen till ändringsdirektiv föreslås också inrättandet av en ny europeisk myndighet för marknaden för elektronisk kommunikation i det nya Telekompaketet i KOM(2007) 699. Detta förslag bortses dock från i den fortsatta framställningen.

¹²² Jfr. regeringens faktapromemoria 2007/08:FPM45.

¹²³ Jfr. KOM(2007) 697 och KOM(2007) 698. Se också regeringens faktapromemoria 2007/08:FPM45.

användningen. Den nya regleringen innehåller också förslag som medför ökade säkerhets- och tillförlitlighetskrav för användningen av kommunikationsnät, en mängd nya konsumenträttigheter och rättigheter för enskilda såsom än hårdare regler för att ytterligare underlätta telefonioperatörsbyte också med bibehållet telefonnummer (nu på en arbetsdag), mer jämförbara prisuppgifter, förbättrad rätt till information om och kring avtal som ger anslutning till ett allmänt kommunikationsnät för konsumenter, möjlighet att ringa gratisnummer mellan medlemsländer, ökat skydd av den personliga integriteten genom upplysningskrav om en operatör misstänker att privat information av någon anledning hamnat i orätta händer, en ökad bredbandstillgång för vissa medborgare företrädesvis genom en förbättrad radiofrekvensanvändning, ett utökat konsumentskydd och förbättringar av användartillgänglighet för personer bl.a. med funktionshinder, regler för att underlätta bekämpandet av skräppost, och effektiviseringar kring det gemensamma europeiska larmnumret (112).¹²⁴

Inte ens i de ursprungliga förslagen från kommissionen finns det således några explicita bestämmelser om att stänga av användare från internet eller reglering av innehåll. Bestämmelser om att en proportionalitetsbedömning ska göras när en stat vill begränsa tillgången till en internetsida lyser också med sin frånvaro. (För att inte tala om bestämmelser som över huvud taget reglerar frågan om, och hur, en stat kan eller ska begränsa internettillgången för sina medborgare.) Likaså finns det inga påbud för (eller förbud mot) att tjänsteleverantörer ska filtrera innehåll, övervaka vad kommunikationstjänsten används till och hur, eller stänga av användare vid brottsmisstanke. Slutligen regleras inte heller några sådana andra aspekter vilka räknades upp i sista stycket i avsnitt 5.1 ovan i kommissionens ursprungliga förslag, eller någon av de efterkommande ändringarna av detsamma. Förslagen har dock som sagt ändå kritiserats i debatten.¹²⁵

5.3 Hadopi och medbeslutandeförfarandet

Innan tvistefrågorna mellan parlamentet och rådet i förslaget till det nya Telekompaketet återges bör först viss bakgrundsfakta återges. Som bekant pågår på många plan, och i många sammanhang, ett arbete mot att förhindra, förebygga och underlätta bekämpandet av pågående immaterialrättsliga och främst upphovsrättsliga intrång på internet.¹²⁶ Samtidigt pågår också ett arbete för att söka tillhandahålla effektiva medel för att förebygga och bekämpa organiserad brottslighet och terrorism via olika former av elektronisk kommunikation, inbegripet internet.¹²⁷

I Frankrike har i ljuset av främst den förstnämnda av dessa aspekter nyligen antagits vad som ofta beskrivs som en av världens hårdaste lagar mot pirat-

¹²⁴ Jfr. KOM(2007) 697 och KOM(2007) 698. Se också regeringens faktapromemoria 2007/08:FPM45.

¹²⁵ Jfr. KOM(2007) 697, KOM(2008) 724, KOM(2007) 698 och KOM(2008) 723.

¹²⁶ Se avsnitt 4 ovan.

¹²⁷ Se avsnitt 6 nedan.

kopiering. Också detta lagförslag, vilket ofta kallas för Hadopi med hänvisning till den myndighet som ska handha ärendena, har varit med om ett flertal turer. Det ursprungliga förslaget fick efter andra försöket majoritet i nationalförsamlingen, men fick bakläxa av den franska författningsdomstolen. Enligt det första förslaget skulle redan internetanvändare som misstänktes begå rättighetsintrång kunna stängas av från internet. Författningsdomstolen slog dock fast att endast en domare kan införa sanktioner mot medborgerliga rättigheter som att avsluta en internetuppkoppling. Det reviderade förslaget gick ut på att den särskilt inrättade myndigheten i ett trestegsförfarande först via e-mail och därefter via vanlig post underrättar och varnar internetleverantören och i förlängningen abonnemangsinnehavaren om att ett rättighetsintrång misstänks ha skett, och därefter med hjälp av en rättslig prövning kan framtvunga en avstängning kombinerat med en svartlistning av en abonnemangsinnehavare från internet i upp till ett år. Efter att det reviderade förslaget nu passerat nationalförsamlingen, senaten och författningsdomstolen i Frankrike väntas det kunna träda ikraft inom en snar framtid. Samtidigt har den brittiska regeringen sagt att liknande sanktioner kan komma att införas i Storbritannien om ett där nyligen infört förfarande med varningsbrev vid rättighetsintrång via internet inte får avsedda effekter.¹²⁸

Rättslig grund för Telekompaketet är artikel 95 EG-fördraget (EGF), och beslutsförfarandet regleras därför av artikel 251 EGF. Beslutsförfarandet enligt denna bestämmelse är invecklat, men bör av snart uppenbara skäl ändå återges i sin helhet.¹²⁹ Kommissionen lägger inledningsvis lagförslag till Europaparlamentet och rådet, och Europaparlamentet ges då möjlighet att föreslå ändringar. Därefter ges rådet möjlighet att anta (det av Europaparlamentet eventuellt ändrade) lagförslaget med kvalificerad majoritet. Om så inte sker ska rådet med kvalificerad majoritet anta en gemensam ståndpunkt med en fullständig redogörelse för dess grunder och delges parlamentet, samtidigt som kommissionen lämnar parlamentet en fullständig redogörelse för sin ståndpunkt angående den föreslagna rättsakten samt de av parlamentet proponerade ändringarna, artikel 251.2 EGF. Därefter ges parlamentet en möjlighet att inom tre månader godkänna den gemensamma ståndpunkten, med absolut majoritet avvisa densamma och därmed förkasta den föreslagna rättsakten, eller med absolut majoritet föreslå ändringar i den gemensamma ståndpunkten. Om det sistnämnda sker ska de föreslagna ändringarna i den gemensamma ståndpunkten återigen delges rådet och kommissionen, och kommissionen ska yttra sig över dessa ändringar, artikel 251.2(a-c) EGF.

¹²⁸ Se exv. Pfanner, *France Approves Wide Crackdown on Net Piracy*, The New York Times 2009-10-22, Phillips, *France Passes Tough Internet Piracy Bill*, BusinessWeek 2009-09-17, TT-AFP, *Fransk lag mot nätpirater godkänd*, Svenska Dagbladet 2009-09-22, TT-AFP, *Nej till fildelningslag i Frankrike*, Dagens Nyheter 2009-06-10, TT-Reuters, *Fortsatt strid om fransk fildelarlag*, Svenska Dagbladet 2009-09-15.

¹²⁹ Förslag har getts om att istället ha artikel 251 EGF i en bilaga till uppsatsen. Detta ställer dock krav på att läsaren kan tillgodogöra sig innebörden i det förfarande som regleras i denna bestämmelse samt, för förståelsen av nästkommande avsnitt, verkligen sätter sig in i processens steg (eller ens läser artikeln). Av denna anledning har jag därför, liksom gjordes med artikel 8 EKMR i kapitel 3 ovan, istället återgett innebörden av bestämmelsen. Jämfört med artikel 251 EGF är denna återgivning åtminstone kortare.

Därefter ges rådet återigen möjlighet att inom tre månader med kvalificerad majoritet godta alla nu föreslagna ändringar och därmed anta rättsakten, om inte kommissionen i sitt yttrande har avstyrkt någon av dessa. Då måste beslut fattas av rådet enhälligt för att anta rättsakten. Om rådet i detta läge inte med kvalificerad majoritet godkänner alla ändringar ska en förlikningskommitté tillsättas, artikel 251.3 EGF. Denna kommitté ska bestå av medlemmar eller företrädare för rådet, samt lika många företrädare för parlamentet. Kommissionen ska också delta i kommitténs arbete, och söka närma parlamentets och rådets ståndpunkter. Kommittén har till uppgift att med kvalificerad majoritet av ledamöterna som företräder rådet samt med majoritet av ledamöterna som företräder parlamentet komma överens om ett gemensamt utkast, artikel 251.4 EGF. Förlikningskommittén har efter att den har sammankallats sex veckor på sig att godkänna ett gemensamt utkast, som därefter måste antas inom ytterligare sex veckor av parlamentet med absolut majoritet och rådet med kvalificerad majoritet. Om något utkast inte godtagits av kommittén inom sex veckor, eller det inte antas av parlamentet och/eller rådet efter sex veckor efter den tidpunkt som ett utkast godtagits av kommittén, förfaller lagförslaget, artikel 251.5-6 EGF. Slutligen kan tidsfristerna i vissa fall förlängas med kortare perioder, artikel 251.7 EGF.

5.4 Tvistefrågorna

Vad som så har hänt vid antagandet av ändringarna i Telekompaketet är följande. Kommissionen lade som sagt fram sina första förslag till ändringar i Telekompaketet till Europaparlamentet och rådet i förslaget till ändringsdirektiv ”bättre reglering” KOM(2007) 697 och ”medborgarnas rättigheter” KOM(2007) 698 den 16 november 2007. Under Europaparlamentets behandling av kommissionens bägge ursprungliga förslag till ny reglering lades en mängd ändringsförslag i olika delar fram. Av dessa antog parlamentet vid sin första behandling av kommissionens förslag den 24 september 2008 126 ändringsförslag för ändringsdirektivet ”bättre reglering” och 155 ändringsförslag för ändringsdirektivet ”medborgarnas rättigheter”.¹³⁰ Av dessa ändringsförslag är det främst ändringsförslag 138 beträffande ändringsdirektivet ”bättre reglering”, och ändringsförslag 166 beträffande ändringsdirektivet ”medborgarnas rättigheter” som har uppmärksamrats i debatten och i media, samt också har varit de största tvisteämnena mellan parlamentet och rådet.

I det nuvarande ramdirektivet sägs i artikel 8.1 att de nationella regleringsmyndigheterna (i Sverige Post- och telestyrelsen) i sin tillsyn och verksamhet enligt regleringen genom att vidta alla rimliga åtgärder också ska uppnå ett flertal mål vilka räknas upp i artikel 8.2-4. I artikel 8.2 återges mål som ska främja konkurrens vid tillhandahållandet av elektroniska kommunikationsnät, i artikel 8.3 mål som ska bidra till utvecklingen av den inre marknaden, och i artikel 8.4 mål som ska främja intressen för medborgarna inom EU. I kommissionens första förslag till ändringsdirektiv ”bättre reglering”

¹³⁰ Jfr. KOM(2008) 724, s. 2, KOM(2008) 723, s. 2.

föreslås ett par förändringar i, och tillägg till, just artikel 8. I parlamentets ändringsförslag 138 föreslogs att ett ytterligare tillägg skulle göras till målen för de nationella regleringsmyndigheterna i artikel 8.4 genom att en ny punkt h skulle tillföras. Denna skulle innebära att de nationella regleringsmyndigheterna ska främja de intressen som medborgarna i Europeiska unionen har också genom att, såsom den svenska översättningen av tillägget lyder, ”tillämpa principen att inga begränsningar i slutanvändarnas grundläggande rättigheter och friheter framför allt enligt artikel 11 i Europeiska unionens stadga om de grundläggande rättigheterna om yttrandefrihet och informationsfrihet får ske utan föregående beslut från rättsvårdande myndigheters sida utom i de fall den allmänna säkerheten hotas då beslut kan fattas i efterhand”.¹³¹

Ändringsförslag 138 riktade sig således inte direkt mot någon av bestämmelserna i den nuvarande regleringen, eller kommissionens förslag till ny reglering. Det ska dock finnas omständigheter som tyder på att ändringsförslaget var en motreaktion av parlamentet på det i avsnitt 5.3 ovan berörda franska lagförslaget som vid denna tidpunkt inte inkluderade en föregående domstolsprövning vid avstängning av franska medborgare från internet. Därtill ska andra ändringsförslag till Telekompaketet i parlamentets första behandling ha lagts av andra parlamentsledamöter (företrädesvis franska) vilka ska ha gett öppningar för en politik med liknande sanktioner mot exempelvis presumtiva illegala fildelare också inom unionen. Dessa ska ha lett till en mängd motförslag från andra ledamöter, inklusive ändringsförslag 138 och 166.¹³²

Ändringsförslag 166 berör å sin sida införandet av en ny artikel 32a i direktivet om samhällsomfattande tjänster och användares rättigheter. Detta förslag säger enligt den svenska översättningen att:

Medlemsstaterna ska se till att eventuella begränsningar av användarnas rätt till tillgång till innehåll, tjänster och tillämpningar, om så krävs, genomförs med hjälp av lämpliga åtgärder i enlighet med principerna om rimliga proportioner, effektivitet och avskräckande verkan. Dessa åtgärder får inte hindra utvecklingen av informationssamhället, i enlighet med Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 [...] (”Direktiv om elektronisk handel”) * , och får inte gå på tvärs mot medborgarnas grundläggande rättigheter, inklusive rätten till ett privatliv och rätten till ett korrekt rättsförfarande”.¹³³

Direktivet om samhällsomfattande tjänster och användares rättigheter innehåller som sagt inga liknande bestämmelser sedan tidigare, och inte heller denna bestämmelse verkar ha varit en direkt reaktion mot kommissionens ursprungliga förslag. Förslaget lades av svenska vänsterpartistiska parlamentsledamoten Eva-Britt Svensson, och avsikten med förslaget ska ha varit

¹³¹ Europaparlamentets lagstiftningsresolution P6_TA(2008)0449 och Europaparlamentets ståndpunkt P6_TC1-COD(2007)0247.

¹³² Jfr. Rosén, *Bakgrund: Striden om Telekompaketet*, Dagens Nyheter 2009-04-27, Rosén, *EU-nej till att stänga av fildelare*, Dagens Nyheter 2009-04-21.

¹³³ Europaparlamentets lagstiftningsresolution P6_TA(2008)0452 och Europaparlamentets ståndpunkt P6_TC1-COD(2007)0248. Asterisken återfinns i originaltexten och är utan förklaring.

att garantera de fri- och medborgerliga rättigheterna på nätet, samt att internet ska vara öppet för alla och att företag inte ska kunna överta myndigheters befogenheter.¹³⁴

I enlighet med medbeslutandeförfarandet vilket beskrevs i avsnitt 5.3 ovan hade rådet härefter möjlighet att anta Telekompaketet med de av parlamentet föreslagna ändringarna. Rådet godtog visserligen många av parlamentets ståndpunkter vid sin behandling. Men varken ändringsförslag 138 eller 166 bifölls, vilket framgår av de bägge gemensamma ståndpunkterna som upprättades av rådet den 16 februari 2009.¹³⁵ Skälen till varför dessa bägge förslag inte kunde godtas framgår inte av rådets officiella dokument. Av det sista parlamentsbetänkandet inför Europaparlamentets tredje läsning framgår det dock att rådet under det första trepartssamtalet efter den andra läsningen angav som skäl att den rättsliga grunden för Telekompaketet (artikel 95 EGF) inte medgav en sådan reglering.¹³⁶ I dagstidningarna framfördes som skäl att den nuvarande regleringen behandlar marknads- och konkurrensfrågor, och att innehållsfrågor och mänskliga rättigheter implicit ska hållas utanför regleringen.¹³⁷ Förfarandet gick därför in i en andra behandling i parlamentet. Inför denna behandling skedde trepartssamtal mellan representanter för rådet, parlamentet och kommissionen för att nå kompromisslösningar om de av parlamentets ändringsförslag som rådet inte biföll. De bägge förslagen till andrabehandlingsrekommendationer av föredragandena i de respektive ansvariga utskotten i parlamentet inför parlamentets andra behandling av Telekompaketet inkluderade därför också flera kompromisser. Beträffande förfarandet för att begränsa en användares tillgång till internet nåddes och godtogs dock aldrig någon kompromiss under utskottsbehandlingen, och ett tillägg till ramdirektivet enligt den ursprungliga lydelsen av ändringsförslag 138 föreslogs och bifölls sedermera i det ansvariga utskottet.¹³⁸

Ett kompromissförslag beträffande denna fråga framlades därefter, men bifölls aldrig av parlamentet när voteringen för den andra behandlingen genomfördes den 6 maj 2009. Istället antog parlamentet också vid sin andra behandling ett identiskt tillägg till ramdirektivet som det ursprungliga ändringsförslag 138. De övriga kompromisslösningarna godtogs dock, och den enda återstående oenigheten mellan parlamentet och rådet var i detta läge därför frågan om förfarandet vid begränsning av tillgång. Beträffande ur-

¹³⁴ Stiernstedt, *Hård slutstrid om Internets framtid*, Dagens Nyheter 2009-04-15.

¹³⁵ Jfr. Rådets gemensamma ståndpunkt 16496/1/08 och 16497/1/08.

¹³⁶ Jfr. betänkande om förlikningskommitténs gemensamma utkast PE430.561v02-00. Det skulle inte vara möjligt att påtvinga medlemsstaterna en särskild rättslig struktur vilken även gäller för brottmål genom artikel 95 EGF, vilket ändringsförslag 138 implicit skulle innebära. Likaså skulle ett krav på ett föregående domstolsbeslut medföra problem för medlemsstater där ett sådant krav inte ställs för att vidta åtgärder mot en enskild. Att kommissionen vid två tillfällen inte funnit några som helst problem med att anta ändringsförslag 138 kommenteras dock inte. Att kompromissen därtill är lika "ingripande" (läs: också redan borde gälla enligt EKMR) har av naturliga skäl inte heller kommenterats av rådet.

¹³⁷ Jfr. Stiernstedt, *Hård slutstrid om internets framtid*, Dagens Nyheter 2009-04-15.

¹³⁸ Numera med beteckningen ändringsförslag 46. Jfr. förslag till andrabehandlingsrekommendation PE420.223 och PE421.119 samt andrabehandlingsrekommendation A6-0272/2009 och A6-0257/2009.

sprungliga ändringsförslag 166 biföll parlamentet således en kompromiss, innebärande att ett nytt skäl infördes i ingressen till direktivet om samhälls-omfattande tjänster och medborgarnas rättigheter samt att ett tillägg till direktivets syfte och tillämpningsområde gjordes.¹³⁹

Följande skäl kommer därför att införas i ingressen till direktivet om samhälls-omfattande tjänster och medborgarnas rättigheter enligt den primära svenska översättningen:

(22) Slut användarna bör kunna bestämma vilket innehåll de vill skicka och ta emot, samt vilka tjänster och tillämpningar och vilken maskinvara och programvara de vill använda för detta ändamål, utan att det påverkar behovet att bevara nätens och tjänsternas integritet och säkerhet. Med en konkurrensutsatt marknad får användarna tillgång till ett brett innehåll och ett stort urval av tillämpningar och tjänster. De nationella regleringsmyndigheterna bör främja användarnas förmåga att skaffa sig tillgång till och distribuera information, samt att använda valfria tillämpningar och tjänster i enlighet med artikel 8 i direktiv 2002/21/EG (ramdirektivet). Med tanke på den ökade betydelsen av elektronisk kommunikation för konsumenter och företag bör användare under alla omständigheter vara fullt informerade om eventuella begränsningar av användningen av elektroniska kommunikationstjänster som införts av tjänstens och/eller nätets leverantör. Leverantören bör ha möjlighet att själv specificera informationen så att den anger antingen vilket slags innehåll, tillämpning eller tjänst det är fråga om, eller de individuella tillämpningarna och tjänsterna, eller bådadera. Beroende på den använda tekniken och vilken begränsning som tillämpas kan dessa begränsningar kräva användarnas samtycke i enlighet med direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation).

I artikel 1, syfte och tillämpningsområde, kommer enligt kompromissen därtill en ny p. 2a att införas:

2a. I detta direktiv varken föreskrivs eller förbjuds villkor som införs av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster och som begränsar användarnas tillgång till och/eller användning av tillämpningar och tjänster, om dessa villkor är tillåtna enligt nationell lagstiftning och stämmer överens med gemenskapsrätten; däremot ges information om sådana villkor. Nationella bestämmelser om slutanvändares tillgång till eller användning av tjänster och tillämpningar över elektroniska kommunikationsnät ska vara förenliga med fysiska personers grundläggande fri- och rättigheter, inklusive rätten till personlig integritet och rätten till ett korrekt rättsförfarande, så som dessa definieras i artikel 6 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

Med kompromissen understryks i direktivet således ytterligare att det varken finns några påbud för eller förbud mot att införa begränsningar av användares tillgång till och användning av tjänster, men att information ska ges om sådana begränsningar.

Kommissionen godtog i sitt yttrande den 29 juli 2009 samtliga av parlamentets föreslagna ändringar (vilka bortsett från frågan om förfarandet vid begränsning av tillgång som sagt var i enlighet med de framförhandlade kom-

¹³⁹ Jfr. Europaparlamentets lagstiftningsresolution P6_TA(2009)0361 och Europaparlamentets ståndpunkt P6_TC2-COD(2007)0247 samt Europaparlamentets lagstiftningsresolution P6_TA(2009)0360 och Europaparlamentets ståndpunkt P6_TC2-COD(2007)0248. Se också kommissionens yttrande KOM(2009) 420 och KOM(2009) 421.

promisserna).¹⁴⁰ Rådets godkände aldrig parlamentets ståndpunkt, och en förlikningskommitté med representanter från rådet och parlamentet tillsattes för att återigen söka nå en överenskommelse om ursprungliga ändringsförslag 138. Den 5 november 2009 tillkännagavs så under en presskonferens att ett gemensamt utkast hade antagits enhälligt av förlikningskommittén.¹⁴¹

Den slutliga kompromissen i den kvarvarande tvistefrågan innebar att ett nytt tillägg i ramdirektivet istället gjordes till artikel 1, och bestämmelsen kommer därför också att gälla för samtliga rättsakter i Telekompaketet. Kompromissen antogs med mycket bred majoritet i parlamentet den 24 november 2009. Enligt kompromissen kommer således i artikel 1 ramdirektivet införas en ny punkt 3a vilken enligt den primära svenska översättningen kommer att lyda:¹⁴²

3a. Åtgärder som vidtas av medlemsstaterna angående slutanvändarnas tillträde till eller användning av tjänster och applikationer genom elektroniska kommunikationsnät ska respektera fysiska personers grundläggande fri- och rättigheter som garanteras genom den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och de allmänna principerna i gemenskapsrätten. Alla dessa åtgärder angående slutanvändares tillgång till eller användning av tjänster och tillämpningar genom elektroniska kommunikationsnät som kan medföra en inskränkning av dessa grundläggande fri- och rättigheter får därför införas endast om de är lämpliga, proportionella och nödvändiga i ett demokratiskt samhälle, och genomförandet av dem ska vara föremål för tillräckliga rättssäkerhetsgarantier i enlighet med den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och med de allmänna principerna i gemenskapsrätten, inbegripet verksamt rättsligt skydd och korrekt rättsförfarande. Följaktligen får dessa åtgärder vidtas endast med vederbörlig respekt för principen om presumtion för oskuld och rätten till integritet. Ett föregående, rättvist och opartiskt förfarande ska garanteras, inbegripet den eller de berörda personernas rätt att höras, med förbehåll för behovet av lämpliga förutsättningar och processuella arrangemang i vederbörligen underbyggda brådsakande fall i enlighet med den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Rätten till effektiv och snabb domstolsprövning ska garanteras.

Genom kompromissen får således användares tillgång exempelvis till internet endast begränsas om dessa åtgärder är ”lämpliga, proportionella och nödvändiga i ett demokratiskt samhälle”, de får endast vidtas ”med vederbörlig respekt för principen om presumtion för oskuld och rätten till integritet” och efter ”ett föregående, rättvist och opartiskt förfarande” som garanterar en ”rätt att höras” samt ”rätten till effektiv och snabb domstolsprövning”. Telekompaketet är således nu antaget, och väntar bara på officiell publicering före det träder ikraft. Tvisten om Telekompaketet kommer att kommenteras mer utförligt i avsnitt 7.3 nedan.

¹⁴⁰ Kommissionens yttrande KOM(2009) 420 och KOM(2009) 421.

¹⁴¹ Rosén, *Kompromiss om telekompaketet klar i natt*, Dagens Nyheter 2009-11-05, Ståhl, *Telekompaketet slutförhandlat*, Svenska Dagbladet 2009-11-05.

¹⁴² Jfr. gemensamt utkast godkänt av förlikningskommittén PE-CONS 3677/09 samt Europaparlamentets lagstiftningsresolution P7_TA-PROV(2009)0068.

5.5 Kritik mot Telekompaketet

Också debatten kring Telekompaketet har varit tämligen långlivad, och har haft inslag av integritetsargument. Flera frågor har redan antytts i tidigare avsnitt i detta kapitel. Avsikten med detta avsnitt, liksom med avsnitt 4.5 ovan, är endast att ge ett par exempel på argument från den omkringgårdande debatten samt hur den har förts och beskrivits i traditionella media. Beträffande i första hand parlamentsbehandlingen av Telekompaketet har en omfattande debatt, samt upplysnings- och opinionsverksamhet också förts på internet.¹⁴³ De frågor som har framställts som grundläggande och varit mest framträdande i debatten tangerar dock inte fullt ut de som har diskuterats mest i den gemenskapsrättsliga lagstiftningsprocessen.

Grundfrågan i Telekompaketet och debatten, samt den politiska tvisten kring detsamma, har således framställts vara om internet ska vara en digital allmänning för alla, som alla har tillgång till och där allt får finnas, eller om internet istället ska eller bör regleras hårdare i fråga om vem som ska få tillgång till nätet, samt vad som ska få finnas där. Denna problemställning har också, i inbördes något varierande former, kallats för ”nätneutralitet”.¹⁴⁴ Nätneutralitetsfrågan (och i förlängningen Telekompaketet) har också sagts handla om tjänsteleverantörernas framtida roll. Om de som huvudregeln är idag endast ska svara och stå för mere conduit – endast tillhandahållandet av ledningarna över vilken kommunikationen sker – eller om de också ska ha ett ansvar för och kunskap om vad deras kunder gör på internet.¹⁴⁵

Över huvud taget ska många av förslagen och stora delar av diskussionen under processen ha handlat om, och haft sin grund i, frågor kring upphovsrätt, illegal fildelning och åtgärder mot sådana brott. Starka intressen från organisationer och enskilda företrädare inom branscher som är beroende av upphovsrätten har skildrats ligga bakom Telekompaketet, och dessa ska genom intensiv lobbying ha ställt krav på hårdare lagstiftning mot piratkopiering inom unionen. Kampen mot terrorismen ska också ha funnits med i bilden. Det har också påståtts att vissa tjänsteleverantörer därtill ska ha haft en vilja att spärra eller reglera tjänster vilka konkurrerar med andra liknande tjänster som de själva redan erbjuder, såsom exempelvis Skype som är ett program för IP-telefoni vilket skulle konkurrera med mer traditionella telefonitjänster som erbjuds av tjänsteleverantören.¹⁴⁶ Beträffande denna sista fråga verkar emellertid av en debattartikel att döma ingen av de största eller

¹⁴³ Se exv. Blackout Europe (<http://blackouteurope.eu>), Iptegrity.com (<http://www.iptegrity.com>), La Quadrature du Net (<http://www.laquadrature.net>), We Rebuild (<http://werebuild.eu>).

¹⁴⁴ Jfr. Olsson, *Bakslag för internetaktivister om telekompaketet*, Svenska Dagbladet 2009-09-28, Rosén, *Internetanvändarens guide till EU:s telekompaket*, Dagens Nyheter 2009-03-31, Stiernstedt, *EU röstar om friheten på nätet*, Dagens Nyheter 2009-03-31.

¹⁴⁵ Rosén, *Bakgrund: Striden om Telekompaketet*, Dagens Nyheter 2009-04-27.

¹⁴⁶ Jfr. Olsson, *Bakslag för internetaktivister om telekompaketet*, Svenska Dagbladet 2009-09-28, Rosén, *Bakgrund: Striden om Telekompaketet*, Dagens Nyheter 2009-04-27, Rosén, *Internetanvändarens guide till EU:s telekompaket*, Dagens Nyheter 2009-03-31, Stiernstedt, *Hård slutstrid om internets framtid*, Dagens Nyheter 2009-04-15.

viktigaste svenska internetleverantörerna vilja gå i denna riktning. Istället görs i denna ett kraftigt ställningstagande mot inskränkningar, ökad övervakning och ett ökat ansvar, och mere conduit förespråkas.¹⁴⁷

Exempel på saker som har sagts regleras i, vara en följd av, eller åtminstone varit på förslag i, det nya Telekompaketet har slutligen varit; att tillgång till webbplatser ska kunna filtreras och/eller blockeras, att en stat som beslutar att stänga av en webbplats ska väga detta mot de begränsningar som detta förorsakar informationssamhället, att tjänsteleverantörer genom regleringen skulle tvingas övervaka och stänga av användare när det föreligger misstanke om brott, att en liknande politik som den som nyligen förts i Frankrike också i övrigt skulle rättfärdigas, samt att regleringen öppnar upp för att tjänsteleverantörer exempelvis kan stycka upp internet och göra så att deras kunder enbart kommer åt sidor eller tjänster som leverantören har avtal med.¹⁴⁸ Över huvud taget nämns den sistnämnda farhågan vid många olika tillfällen, och i många olika sammanhang. Telekompaketet skulle således bestämma internets form och innehåll, och regleringen skulle leda till ett indelat internet som kan liknas vid kabelteve som en metafor för den tidigare beskrivna uppstyckningen där användaren får betala för vad den vill ha, och klara sig utan resten.¹⁴⁹ En orsak till denna sista farhåga samt varför de ursprungliga ändringsförslagen 138 och 166 särskilt behövs, skulle vara att vissa bestämmelser i Telekompaketet antyder att internetleverantörer enbart ska garantera tillgängligheten till legalt innehåll, samt att formuleringarna öppnar upp för att enskilda kan komma att uteslutas från nätet.¹⁵⁰

Flera av dessa ämnen och bekymmer har redan behandlats och/eller besvarats i kapitlets tidigare avsnitt. Generellt kan dock sägas att risken för att farhågorna i de flesta fall skulle förverkligas varit tämligen låg eftersom det antingen varit fråga om saker som över huvud taget aldrig varit på tal i lagstiftningsprocessen, eller förslag som fått en stor medial spridning, men som inte fått ett särskilt stort gehör i det ifrågavarande politiska organet.¹⁵¹ Med detta sagt, är frågorna som farhågorna i sig berört allvarliga (och intressanta). Beträffande nätneutralitet sägs i de artiklar som nämner detta begrepp om vartannat att parlamentets ursprungliga ändringsförslag 138 och/eller 166 bl.a. skulle trygga dessa problem. Såsom förslagen varit utformade, och nätneutralitetsfrågan beskrivs, är det dock inte fråga om helt likartade ting.¹⁵²

¹⁴⁷ Fransson m.fl., *Nätoperatörernas roll görs omöjlig*, Brännpunkt, Svenska Dagbladet 2009-09-30.

¹⁴⁸ Jfr. Olsson, *Telekompaketet ska öka konsumenternas rättigheter*, Svenska Dagbladet 2009-05-04, Rosén, *Internetanvändarens guide till EU:s telekompaket*, Dagens Nyheter 2009-03-31, Rosén, *Liberalit sidbyte stoppade Telekompaketet*, Dagens Nyheter 2009-05-06, Stiernstedt, *Hård slutstrid om internets framtid*, Dagens Nyheter 2009-04-15, Svahn, *Telekompaketet: Strid om rättssäkerhet in i det sista*, Dagens Nyheter 2009-05-05.

¹⁴⁹ Jfr. Olsson, *Telekompaketet ska öka konsumenternas rättigheter*, Svenska Dagbladet 2009-05-04, Stiernstedt, *”En krigsförklaring mot internet”*, Dagens Nyheter 2009-04-16, Stiernstedt, *Hård slutstrid om internets framtid*, Dagens Nyheter 2009-04-15.

¹⁵⁰ Carp, *IT-branschen: ”Telekompaketet behöver tillägg om mänskliga rättigheter”*, Dagens Nyheter 2009-05-05.

¹⁵¹ Läs: Europaparlamentet.

¹⁵² Jfr. avsnitt 5.4 ovan.

Till sist har naturligtvis frågan om rätten till domstolsprövning vid exempelvis begränsning av tillgång berörts i på det hela taget samtliga artiklar som nämnts i noterna ovan. Här har kopplingen till striden mellan Europaparlamentet och rådet också varit störst. Intressant är dock att det enbart tycks vara denna fråga som uppmärksammas i den omkringgårdande debatten. Frågan om proportionalitet och rimlighet i att begränsa personers tillgång till internet som en sanktion på (t.o.m. misstänkta) immaterialrättsliga rättighetsintrång vilka har begåtts via internet verkar inte ha uppmärksammas. I denna fråga finns det också stora integritetsaspekter. Denna fråga återkommer i den avslutande diskussionen.

6 Datalagringsdirektivet

Den 15 mars 2006 antogs Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät. Detta direktiv var redan när det antogs kontroversiellt ur integritetssynpunkt, och debatten kring det lever i allra högsta grad också idag. I detta uppsatsens sista huvudsakligen deskriptiva kapitel ska därför datalagringsdirektivet (vilket direktivet har kommit att kallas) samt dess syfte närmare presenteras. Implementeringen av direktivet i svensk rätt har ännu inte skett. Ett utredningsbetänkande med förslag på hur direktivet ska genomföras lades dock fram redan under 2007. Vad som har framkommit om den svenska implementeringen ska inte desto mindre också återges i detta kapitel. Slutligen ska något sägas om några av de invändningar som har rests gentemot direktivet, samt direktivets förhållande till det i kapitel 4 ovan berörda civilrättsliga sanktionsdirektivet.

6.1 Allmänt om direktivet

Datalagringsdirektivet ålägger medlemsstaterna att anta bestämmelser för att säkerställa att vissa data som genereras vid elektronisk kommunikation sparas för att underlätta den straffrättsliga processen i vid mening i förhållande till vissa grövre brott. Också datalagringsdirektivet antogs med stöd av artikel 95 i EG-fördraget, och finner av denna anledning dock sin yttersta motivering i att undandöra hinder på den inre marknaden. Av ingressen till datalagringsdirektivet framgår det således att det enligt direktivet om integritet och elektronisk kommunikation¹⁵³ är möjligt för medlemsstaterna att införa lagstiftning om en skyldighet för tjänsteleverantörer att lagra vissa trafikuppgifter bl.a. för att förebygga, utreda, avslöja och åtala brott, samt att så också gjorts i många medlemsländer. Dessa nationella bestämmelser ska dock ha företett stora skillnader såväl rättsligt som tekniskt. Dessa skillnader ansågs utgöra hinder för den inre marknaden för elektronisk kommunikation eftersom tjänsteleverantörerna ställs inför olika krav i de olika medlemsstaterna avseende vilka uppgifter som ska lagras, längden på lagringstider, samt vilka villkor som ska gälla för lagringen också i övrigt. Datalagringsdirektivets syfte är därför att harmonisera medlemsstaternas reglering av tjänsteleverantörers skyldighet att lagra vissa trafikuppgifter *och säkerställa att de är tillgängliga* för utredning, avslöjande och åtal av allvarliga brott för de brottsbekämpande myndigheterna.¹⁵⁴

¹⁵³ Vilket är direktiv 2002/58/EG, som berörs på ett flertal ställen i både avsnitt 4 och 5 ovan såsom grund för bl.a. den svenska lagen om elektronisk kommunikation och del i Telekompaketet.

¹⁵⁴ Jfr. SOU 2007:76, s. 17, 43, 47f. Det av mig ovan kursiverade syftet med datalagringsdirektivet motiveras inte i direktivets ingress i förhållande till art. 95 EGF. Direktivets lagenlighet i förhållande till EGF har dock prövats av EGD, se avsnitt 6.4 nedan.

Av ingressen till direktivet framgår det också att omfattningen av den elektroniska kommunikationen har ökat avsevärt, och att det både genom forskning och genom medlemsstaternas praktiska erfarenhet framkommit att uppgifter såsom trafik- och lokaliseringssuppgifter om användningen av sådan kommunikation är viktiga för att kunna avslöja, utreda och åtala brott – särskilt vad gäller organiserad brottslighet. Arbetet med direktivet inleddes efter Europeiska rådets uttalande om kampen mot terrorismen som föranleddes av bombattentaten mot tre järnvägsstationer i Madrid den 25 mars 2004, och Sverige var vid denna tidpunkt ett av de drivande länderna i arbetet. Det kan också nämnas att Europeiska rådet efter bombdåden i kollektivtrafiken i London den 7 juli 2005 upprepade vikten av gemensamma åtgärder om lagring av telekommunikationsuppgifter.

6.2 Innebörden av direktivet

Datalagringsdirektivet gäller för trafik- och lokaliseringssuppgifter om både fysiska och juridiska personer samt uppgifter som därutöver är nödvändiga för att kunna identifiera en abonnent eller registrerad användare. Däremot omfattas inte innehållet i elektronisk kommunikation av direktivets tillämpningsområde, artikel 1.2. Lagringsskyldigheten gäller för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller kommunikationsnät, och leverantörernas lagringsskyldighet omfattar uppgifter som dessa antingen genererar genom, och/eller behandlar i, den tjänst som levereras, artikel 3.1. Lagringsskyldigheten omfattar också missade uppringningsförsök, däremot ställer direktivet inga krav på lagring av uppgifter om samtal som inte kopplats fram, artikel 3.2. De trafikuppgifter som ska lagras (och som tjänsteleverantören antingen genererar eller behandlar) framgår av direktivets artikel 5. De är sorterade efter uppgifter som är nödvändiga för att; 5.1(a) spåra och identifiera en kommunikationskälla, 5.1(b) identifiera slutmålet för en kommunikation, 5.1(c) identifiera datum, tidpunkt och varaktighet för en kommunikation, 5.1(d) identifiera typen av en kommunikation, 5.1(e) identifiera användarnas kommunikationsutrustning eller den utrustning som de tros ha använt, och 5.1(f) identifiera lokaliseringen av mobil kommunikationsutrustning.¹⁵⁵

För såväl fast som mobil telefoni ska det uppringande telefonnumret, de nummer som slagits och nummer som samtalet styrts till, namn och adress för abonnent eller registrerad användare för respektive telefonnummer, tid och datum då kommunikationen påbörjades och avslutades, den typ av telefonitjänst som använts samt det uppringande och det uppringda telefonnumret lagras. För mobiltelefoni ska därtill den uppringande och/eller den upp-

¹⁵⁵ Se också SOU 2007:76, s. 123ff. I korthet sägs i SOU:n att de trafikuppgifter som ska lagras enligt direktivet är sådana som genereras eller behandlas vid kommunikation via fast och mobil telefoni, internettelefoni, e-post samt vid internetåtkomst och som svarar på frågorna vem som kommunicerat med vem, vid vilken tidpunkt, var personerna befann sig samt vilken typ av kommunikation som använts, SOU 2007:76, s. 17.

ringda partens IMSI- och IMEI-nummer,¹⁵⁶ vid förbetalda anonyma tjänster datum och tid för den första aktiveringen av tjänsten och den lokaliseringsbeteckning (cell-id)¹⁵⁷ från vilken tjänsten aktiverades, samt lokaliseringsbeteckning (cell-id) för kommunikationens början samt uppgifter som anger cellernas geografiska placering genom referens till deras lokaliseringsbeteckning under den period som kommunikationsuppgifterna lagras, artikel 5. Begreppet telefoni definieras i artikel 2.2(c), och omfattar utöver uppringning och röstsamtal; röstmeddelanden, konferenssamtal, datatelefoni, s.k. extratjänster vilka bl.a. inkluderar omstyrning och överflyttning av samtal, samt meddelandeförmedling och multimedietjänster vilket bl.a. inkluderar SMS, EMS och MMS.¹⁵⁸

För internettelefoni, e-post och internetåtkomst ska tilldelad användaridentitet, eventuella ytterligare användaridentiteter och/eller telefonnummer vilka tilldelats kommunikationen i det allmänna telenätet, namn och adress för abonnent eller registrerad användare för IP-nummer, användaridentitet och/eller telefonnummer som tilldelats vid tidpunkten för kommunikationen, tid och datum för inloggning i och utloggning från den ifrågavarande tjänsten¹⁵⁹ och beträffande internetanslutning tillsammans med tilldelad IP-adress, samt slutpunkt för kommunikationens avsändare¹⁶⁰ lagras. Beträffande e-post och internetbaserad telefoni ska därutöver användaridentitet och/eller telefonnummer som tilldelats de avsedda mottagarna, samt namn och adress för abonnenten/-erna eller den eller de registrerade användarna för den avsedda mottagaren lagras, artikel 5.¹⁶¹ E contrario kan således klart fastställas att vid internetanslutning ska samtliga IP-adresser som abonnentens IP-adress har anslutit eller sökt ansluta till *inte* lagras. Inte heller IP-

¹⁵⁶ Detta är naturligtvis tekniska akronymer. IMSI-numret är ett unikt nummer som finns lagrat på och kan sägas vara kopplat till SIM-kortet i en mobiltelefon. IMEI-numret är ett unikt nummer för mobiltelefonen i sig, och således konstant och oberoende av vilket telefonnummer och/eller SIM-kort som används i mobiltelefonen. Som kuriosum kan nämnas att detta sista nummer på nästan alla mobiltelefoner kan ses genom att knappa in *#06# i telefonen. I den föreslagna svenska regleringen har akronymerna ersatts med begreppen abonnemangsidentitet och utrustningsidentitet. Jfr. SOU 2007:76, s. 304.

¹⁵⁷ Med lokaliseringsbeteckning och cell-id avses identiteten för den cell varifrån ett mobilsamtal påbörjats eller avslutats, artikel 2.2(e). I ren svenska: den basstation som telefonen hade kontakt med, tillsammans med geografiska uppgifter om var denna basstation befinner sig. I den föreslagna svenska regleringen ersätts begreppet med lokaliseringsinformation, vilket är ett mer förståeligt begrepp. Jfr. SOU 2007:76, s. 304.

¹⁵⁸ Se också SOU 2007:76, s. 124ff. Vad SMS är torde de flesta känna till. EMS är en utvidgning av SMS som bl.a. gör att meddelanden längre än 160 tecken kan skickas. MMS är en (något) nyare meddelandeform för mobiltelefoner varmed man utöver text kan skicka ljud, musik, bilder m.m.

¹⁵⁹ Således kan/ska separata tider lagras för internetanslutning, anslutning till e-posttjänster samt anslutning till internettelefonitjänster.

¹⁶⁰ I bestämmelsen talas om uppringande telefonnummer för s.k. uppringda förbindelser (varmed främst torde avses de i Sverige numera allt mer sällan använda analoga telefonmodemen) samt ”DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare”. Dessa bägge bestämmelser sorterar under artikel 5.1(e) vilka som sagt skulle vara uppgifter som är nödvändiga för att identifiera användarnas kommunikationsutrustning eller den utrustning som de tros ha använt. Troligtvis är det detta man avser också med den sista bestämmelsen. DSL är i sig en teknik för snabbare digital överföring av data via (tele)koppartråd.

¹⁶¹ Se också SOU 2007:76, s. 124ff.

adresser vilka anslutit eller sökt ansluta till abonnentens IP-adress omfattas av lagringsskyldigheten av denna anledning. Detta utesluter således att exempelvis lagring av alla webbplatser som en internetanvändare besökt omfattas av lagringsskyldigheten enligt direktivet.¹⁶²

Lagringstiden för uppgifterna ska under normala omständigheter enligt direktivet vara mellan sex månader och två år, artikel 6 och 12. Vissa närmare omständigheter kring hur uppgifterna ska lagras och skyddas anges också i direktivet, däremot inte hos vem. Uppgifterna ska lagras på ett sådant sätt att de utan dröjsmål kan överföras till de behöriga myndigheterna när så begärs (artikel 8), och vissa villkor om de lagrade uppgifternas kvalitet, datasäkerhet och uppgiftsskydd uppställs, artikel 7. Uppgifterna ska förstöras vid slutet av lagringstiden, artikel 7(d). I direktivet regleras slutligen inte frågor kring när och under vilka förutsättningar brottsbekämpande myndigheter ska få tillgång till de lagrade uppgifterna.¹⁶³

6.3 Den svenska implementeringen

Datalagringsdirektivet skulle ha varit implementerat i svensk rätt senast den 15 september 2007, bortsett från lagring av uppgifter om internetåtkomst, internettelefoni och e-post vilka Sverige förbehållit sig att implementera senast den 15 mars 2009, direktivets artikel 15. Som också berördes främst i avsnitt 4.2 ovan finns det i dagsläget ingen skyldighet för leverantörer av allmänna kommunikationstjänster och kommunikationsnät att spara på dylik information i Sverige, och Sverige uppfyller därför inte sina förpliktelser gentemot unionen.¹⁶⁴ Implementeringen verkar dock dröja ytterligare.

Som sagt lades ett utredningsbetänkande med förslag på hur den svenska implementeringen av direktivet ska utformas fram redan i november 2007. I maj 2009 började vad som med mycket stor sannolikhet var ett äkta utkast till lagrådsremiss för den svenska implementeringen cirkulera på internet, om än dess förekomst dementerades av justitiedepartementet.¹⁶⁵ Kort därefter stämde Sverige av kommissionen för att inte ha implementerat direktivet i tid,¹⁶⁶ och av en av regeringens skrivelser till EG-domstolen ska det ha framgått att en proposition avsetts läggas fram under hösten 2009, med ett ikraftträdande av en svensk implementering någon gång under våren 2010. I oktober 2009 sade justitieminister Beatrice Ask till TT dock att någon proposition inte kommer att läggas före riksdagsvalet 2010, bl.a. eftersom frågan är politiskt känslig och för att avvakta en annan utredning vilken ser

¹⁶² En annan sak är att sådan verksamhet bedrivs i Sverige. Klambergers artikel beskriver denna verksamhet bra.

¹⁶³ Se också SOU 2007:76, s. 221ff.

¹⁶⁴ Se också SOU 2007:76, s. 17f, 43f.

¹⁶⁵ Jfr. Johannisson, *Opublicerad lagrådsremiss om ip-adresser tillbakavisas*, Svenska Dagbladet 2009-05-15. I internetversionen av artikeln länkas också till dokumentet.

¹⁶⁶ Olsson, *Sverige stäms för datalagring*, Svenska Dagbladet 2009-05-26.

över polisens arbetsmetoder och hur de utredande myndigheterna ska få tillgång till de lagrade uppgifterna.¹⁶⁷

Det finns ingen anledning till att här spekulera i hur den framtida svenska implementeringen av datalagringsdirektivet därför kan komma att se ut (eller om den ens kommer att ske). Vissa grundläggande frågor såsom lagringsskyldighetens omfattning och lagringstiden skiljer sig också delvis åt mellan utredningsförslaget och den läckta lagrådsremissen. Vad som kan konstateras är dock att ändringar i den nuvarande lagen om elektronisk kommunikation krävs för att den i avsnitt 6.2 ovan beskrivna lagringsskyldigheten ska gälla i Sverige. Enligt de nu gällande bestämmelserna i lagen om elektronisk kommunikation ska t.ex. trafikuppgifter enligt huvudregeln utplånas eller aidentifieras när de inte längre behövs för att överföra ett elektronisk meddelande, 6 kap. 5 §. Undantag görs bl.a. för när uppgifterna behövs för fakturering, när det finns samtycke från abonnenten i vissa fall, tvistlösning, verkställighet av beslut om hemlig teleavlyssning- eller övervakning, samt för åsidosättande av nummerpresentationsskydd när det gäller telefonsamtal för att identifiera störande samtal eller vid nödsamtal, 6 kap. 6, 8 och 13 §§. De nuvarande möjligheterna för brottsbekämpande myndigheter att begära ut information från tjänsteleverantörer är således avhängigt att dessa uppgifter (fortfarande) finns lagrade, under dessa förutsättningar.¹⁶⁸

Som sagt berörs inte frågor kring under vilka förutsättningar de lagrade uppgifterna ska ges ut till brottsbekämpande myndigheter i direktivet. Några utvidgningar av dessa svenska regler, vilka främst återfinns i bestämmelserna om teleövervakning i 27 kap. 19 – 21 §§ rättegångsbalken samt i förutsättningarna för att lämna ut trafik- och kataloguppgifter vid brott jämte 6 kap. 22 § 1 st. lagen om elektronisk kommunikation, torde därför inte krävas vid en framtida svensk implementering. Det kan också tilläggas att det i utredningsbetänkandet inte heller förslogs några ändringar av de nuvarande reglerna i detta avseende. Dessa frågor utreds som sagt för närvarande istället dock av den s.k. polismetodutredningen.¹⁶⁹ Som bekant omfattas i dagsläget bara brott som har ett minimistraff på 6 månader i straffskalan av regleringen i rättegångsbalken. Uppgiftsutlämning enligt lagen om elektronisk kommunikation kan som berördes i avsnitt 4.2 ovan bara ske till däri uppräknade myndigheter, och kräver misstankar om brott med minst två års fängelse i straffskalan. Framtiden får således utvisa när, hur och om datalagringsdirektivet kommer att införlivas i svensk rätt. Under förutsättning att direktivet inte ändras eller upphävs kommer Sverige dock att fällas av EGDomstolen om ett genomförande fortfarande inte har skett när ärendet väl kommer upp till prövning.

¹⁶⁷ TT, *Regeringen skjuter på datalagring*, Svenska Dagbladet 2009-10-21. Det är för övrigt polismetodutredningen som avses.

¹⁶⁸ SOU 2007:76, s. 54ff, 222. Detsamma gäller som bekant också för rättighetshavare som söker få information överlämnad genom informationsföreläggandeinstitutet, jfr. avsnitt 4.2 och 4.6 ovan.

¹⁶⁹ SOU 2007:76, s. 56ff, 227ff.

6.4 Kritik mot direktivet

Datalagringsdirektivet har varit kontroversiellt, på många olika plan, i princip ända sedan den process som ledde fram till dess antagande inleddes. På samma sätt som gjordes i avsnitten 4.5 och 5.5 ovan syftar också detta avsnitt till att ge ett par exempel på den kritik som framförts, i detta fall mot datalagringsdirektivet. Till att börja med var den rättsliga grunden för datalagringsdirektivet omstridd när direktivet antogs. Det förslag som i slutändan blev det nuvarande datalagringsdirektivet var från början avsett att antas som ett rambeslut med rättslig grund i det polisiära och straffrättsliga samarbetet under EU:s tredje pelare. Som bekant antogs det i slutändan som ett direktiv i enlighet med artikel 95 EGF (se avsnitt 6.1 ovan), och med kvalificerad majoritet i rådet.¹⁷⁰

Detta gillades inte av Irland, varmed också Slovakien instämde (som också råkar vara de bägge länder vilka röstade mot direktivets antagande i rådet), och begärde efter antagandet att EG-domstolen skulle ogiltigförklara direktivet för att det inte antagits på korrekt rättslig grund. Man menade bl.a. att direktivets tyngdpunkt snarare låg på att underlätta utredning, avslöjande och åtal av brott än tillnärmning av lagstiftning för att den inre marknaden ska fungera bättre. I EG-domstolens avgörande som kom den 2 oktober 2009 fastslogs dock att den rättsliga grunden för direktivet inte var felaktig. Därvid togs bl.a. fasta på att direktivet uttryckligen undantog frågor om tillgången till uppgifterna eller hur dessa får användas av de rättsliga myndigheterna i medlemsländerna. EG-domstolen underströk i sin dom också att talan endast avsåg valet av rättslig grund för direktivet och att det i ärendet inte påståtts att direktivet skulle innebära ett eventuellt åsidosättande av grundläggande rättigheter.¹⁷¹

På ett lägre och mer nationellt plan konstateras redan i utredningen att den föreslagna uppgiftslagringen är integritetskränkande, och att redan det allmännas säkrande av tillgången till uppgifterna genom lagringen har en påverkan på enskildas integritetsskydd och upplevelse av integritetsintrång. I utredningen konstateras också att det är fråga om ett mycket stort antal trafikuppgifter som varje dygn kommer att lagras, att fler uppgifter kommer att lagras och under en längre tid än idag, samt att endast en ytterst liten del av samtliga dessa uppgifter kommer att användas för de brottsbekämpande syftena. Därtill konstateras att trafikuppgifter i många fall är uppgifter om enskildas personliga förhållanden och korrespondens, och att ett utlämnande av trafikuppgifter för utredning om brott är särskilt känsligt ur integritetssynpunkt. Emellertid sägs i utredningen dessutom att genomförandet av direktivet också kan sägas öka förutsättningarna för en högre grad av säkerhet för enskilda genom att enhetliga bestämmelser införs om vad som ska lagras samt under vilken tid och på vilket sätt detta ska ske.¹⁷²

¹⁷⁰ Jfr. EG-domstolens dom C-301/06. Beträffande sista meningen, jfr. medbeslutandeförfarandet i avsnitt 5.3.

¹⁷¹ Jfr. EG-domstolens dom C-301/06.

¹⁷² SOU 2007:76, s. 109ff.

En hearing om integritetsfrågor genomfördes också av utredningen. Vid denna framfördes bl.a. att det i första hand är vetskapen om att uppgifter finns lagrade, kan tas fram och granskas, samt risken för att de läcker ut till obehöriga, som är de allvarliga bekymren ur integritetssynpunkt. Regleringen troddes också kunna få en psykisk inverkan innebärande att tron till myndigheterna påverkas, människor blir rädda och misstänksamma, samt att de upplever att de lever i ett kontrollsamhälle. Att en ökad informationsmängd leder till ökad risk för att information läcks eller sprids till obehöriga framfördes också. Slutligen poängterades risken för ändamålsglidning. När uppgifterna väl finns till hands kan de lätt börja användas för allt fler syften.¹⁷³

Kritiken som har framförts i de traditionella medierna har berört liknande ämnen; övergripande integritetsproblematik, pris- och kostnadsfrågor, risken för missbruk och läckor, samt att uppgiftslagringen strider mot grundläggande rättigheter vilka skyddas av EKMR och/eller RF. Således har Advokatsamfundets generalsekreterare Anne Ramberg framfört att ett paradigmskifte har skett när man nu ska börjar övervaka och registrera människor som inte är misstänkta för brott. Hon uttalade på samma sätt att det med hjälp av den information som lagras blir väldigt lätt att kartlägga enskilda individers liv och skapa en fullständig bild över vilka personer en individ har haft kontakt med och när. Av andra har det framförts att det är en rättighet att inte få uppgifter gällande sitt privatliv registrerade, och det oavsett ”mjöl i påsen”. Också datainspektionen har beträffande den personliga integriteten understrukt att de, tillsammans med övriga europeiska dataskyddsmyndigheter, har varit starkt kritiska till datalagringsdirektivet.¹⁷⁴

Beträffande skyddade grundläggande rättigheter har framförts att lagringen riskerar att bryta mot RF och EKMR, och i några fall mer specifikt att det ingrepp som sker genom lagringen inte är effektivt eller står i proportion till det man uppnår.¹⁷⁵ Som sagt har också risken för missbruk av de uppgifter som lagrats framhållits. Exempelvis har sagts att det inte finns några garantier för att det inte uppstår några läckor av den lagrade informationen. I direktivet sägs också att informationen enbart får användas vid allvarliga brott, men farhågor kring att detta begrepp missbrukas och tänjs har också framförts.¹⁷⁶

¹⁷³ SOU 2007:76, s. 111f.

¹⁷⁴ Olsson, *Brott mot svensk grundlag?*, Svenska Dagbladet 2008-12-12, Olsson, *Grönt ljus för datalagring*, Svenska Dagbladet 2009-02-10, SvD.se, *Lagen om datalagring upprör*, Svenska Dagbladet 2008-12-13.

¹⁷⁵ Olsson, *Brott mot svensk grundlag?*, Svenska Dagbladet 2008-12-12, Olsson, *Datalagring får tyskar att sluta ringa*, Svenska Dagbladet 2008-12-17, Olsson, *”Sverige bryter mot de mänskliga rättigheterna”*, Svenska Dagbladet 2009-02-11, Svantesson, *”Vi har inget att välja på”*, Dagens Nyheter 2009-05-15. Jfr. avsnitt 3.4 ovan vilka krav som ställs på inskränkningar av artikel 8 EKMR.

¹⁷⁶ Olsson, *Brott mot svensk grundlag?*, Svenska Dagbladet 2008-12-12, Olsson, *Datalagring får tyskar att sluta ringa*, Svenska Dagbladet 2008-12-17.

Slutligen har, av förklarliga skäl i första hand från teleoperatörernas sida, också framförts många ekonomiska invändningar. Denna fråga handlar om vem som ska stå för de kostnader som är nödvändigt förbundna med den införda lagringsskyldigheten – staten eller operatörerna. Kortfattat kan inställningen hos telekombolagen sägas vara att de inte vill betala för en lag de inte ens vill ha själva. I utredningen uppskattas implementeringskostnaden hamna på runt 200 milj kr, och operatörerna föreslås stå för dessa kostnader själva. Samtidigt uppskattar branschorganisationen IT- och telekomföretagen att engångsinvesteringskostnaderna för Sverige lågt räknat kommer att uppgå till 760 milj kr, samt därefter drifts- och underhållskostnader om runt 133 milj kr årligen i dagens penningvärde. Effekterna för mindre operatörer tros också kunna bli förödande. Implementeringskostnaderna för dessa blir relativt högre. Därutöver tolkas direktivets krav på att de lagrade uppgifterna ska utlämnas utan dröjsmål i utredningsförslaget som att detta ska ske med några timmars varsel oavsett tid på dygnet, vilket mindre operatörer med ett fåtal anställda inte heller skulle klara av.¹⁷⁷

I ett par svenska tjänsteleverantörers remissvar på den svenska utredningen förs liknande tankegångar. I Telias remissvar framhålls således att kraven på lagring av uppgifter inte tillför verksamheten något mervärde, och att utgångspunkten därför måste vara att staten ska bära kostnaderna för de åtgärder som måste vidtas för lagringen och utlämningen.¹⁷⁸ I internetoperatören Bahnhof's remissvar framhålls att vi i Sverige av tradition alltid haft ett system som speglar och bygger på antagandet att en åtalad person är oskyldig till dess motsatsen bevisats genom att det krävts misstanke om brott för att ingripa i den personliga integriteten. Med den uppgiftslagring som föreslås ske omvänds normsystemet, alla antas vara skyldiga till något, och alla medborgare övervakas ständigt. Därtill framhävs att det med rimliga tekniska kunskaper enkelt går att dölja sina spår på internet, särskilt med den utformning som uppgiftslagringen fått i direktivet och det föreslagna svenska genomförandet. Resultatet blir då också att de som sannolikt inte har för avsikt att begå brott övervakas minutiöst, medan de med brottsliga avsikter särskilt med kännedom om den ständiga övervakningen förblir osynliga. Slutligen framhävs att inget elektroniskt system kan garanteras vara fullständigt säkert från obehörig tillgång. De uppgifter som avses lagras kan användas för att kartlägga enskilda användares vanor in i minsta detalj. Intrångsriskerna har också en inverkan på uppgifternas användbarhet och tillförlitlighet i rättegångar och förundersökningar.¹⁷⁹

¹⁷⁷ Olsson, *Datalagring kan kosta 1 miljard*, Svenska Dagbladet 2008-12-12, Olsson, *Ingen datalagring före sommaren*, Svenska Dagbladet 2009-06-12, SvD.se, *Lagen om datalagring upprör*, Svenska Dagbladet 2008-12-13, Stenberg, *Nya IT-lagar kostar hushållen miljarder*, Dagens Nyheter 2008-11-30.

¹⁷⁸ TeliaSoneras remissvar över Trafikuppgiftsutredningens betänkande Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76).

¹⁷⁹ Bahnhof remissyttrande SOU 2007:76.

6.5 Datalagring kontra Ipred

Som berördes i avsnitt 6.3 ovan ska trafikuppgifter enligt huvudregeln i lagen om elektronisk kommunikation utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande. Som berördes i avsnitt 4.2 ovan åläggs ingen att spara på den information som kan bli föremål för ett informationsföreläggande enligt informationsföreläggandeinstitutet vilket är en del av den svenska implementeringen av Ipred. Och som slutligen berördes i avsnitt 4.6 ovan lade ett flertal svenska internetleverantörer en kort tid efter genomförandet av Ipred om sina interna rutiner så att trafikuppgifter inte längre behövdes sparas under en mer bestående tid – vilket fick till resultat att det beträffande dessa leverantörer vanligen inte heller finns någon information att lämna ut med hjälp av informationsföreläggandeinstitutet (och detsamma gäller för de svenska rättsliga myndigheterna i dessa fall, jfr. avsnitt 6.3 ovan).

En lättförståelig problematik kan här skönjas. Frågan är således om tjänsteleverantörerna (under förutsättning att datalagringsdirektivet genomförs i Sverige) när de nu blir tvungna att separat lagra sådana uppgifter de idag av olika skäl raderar, därmed genom informationsföreläggandeinstitutet i de immaterialrättsliga lagarna kan bli tvungna att till andra privata aktörer utlämna sådan information som nu trots allt lagras, enkom pga. den framtvingade lagringen. I detta kapitel avslutande avsnitt ska en trolig lösning på denna problematik presenteras.¹⁸⁰

I många olika sammanhang har olika uppfattningar framförts i denna fråga. Åsikterna på den ena sidan bygger vidare på det faktum att de operatörer som tidigare sett till att ”slippa undan” ett utlämnande genom att radera information som inte längre behövs internt nu trots allt kommer att bli skyldiga att spara bl.a. abonnentuppgifter. Eftersom dessa uppgifter nu finns lagrade, ska därmed också en rättighetshavare som lyckas göra sannolikt att exempelvis en viss IP-adress använts vid ett upphovsrättsintrång via internet kunna få denna information överlämnad eftersom den som sagt nu faktiskt finns kvar.¹⁸¹ Från den motsatta sidan har framförts att de uppgifter som kommer att tvångsmässigt lagras i enlighet med genomförandet av direktivet är förbehållet enkom brottsbekämpande myndigheter. Därtill ska datalagringsdirektivet, och/eller den svenska implementeringen, innebära att också de uppgifter som (i mer fakultativ mening) sparas av tjänsteleverantörerna idag, och som är de som idag kan begäras ut med informationsföreläggande-

¹⁸⁰ Frågetecknen har rests kring varför detta avsnitt inte återfinns i den avslutande diskussionen. I kapitel 7 diskuteras i första hand integritetsfrågor, den fråga som diskuteras i detta avsnitt är huvudsakligen av juridisk karaktär. Frågan skulle visserligen också kunna diskuteras i det kapitel som Ipred behandlas i, men eftersom datalagringsdirektivet nu avhandlas efter Ipred har jag valt att förlägga detta avsnitt här.

¹⁸¹ Jfr. den icke namngivna polischefens uttalande i Svantesson, ”*Vi har inget att välja på*”, Dagens Nyheter 2009-05-15. I artikeln återges därefter följande citat; ”När det blir svensk lag har ju faktiskt operatörerna, i enlighet med lagen, skyldighet att spara abonnentuppgifterna i sex månader (om det bli beslutet[sic!] i domstol). Jag tror inte, såsom vissa riksdagsmän säger, att Ipred inte kommer att påverkas av datalagringsdirektivet”.

institutet, i framtiden (eller egentligen redan nu) ska vara förbehållna de rättsliga myndigheterna.¹⁸²

För datalagringsdirektivets del kan denna fråga möjligen till viss del sägas vara öppen. Vilket berördes i avsnitt 6.1 ovan är direktivets syfte att harmonisera och säkerställa att vissa trafikuppgifter lagras för utredning, avslöjande och åtal av allvarliga brott för de nationella brottsbekämpande myndigheterna. Det är för dessa syften som en tvångsmässig lagring ska ske. Direktivet innehåller som sagt inga omfattande eller utförliga bestämmelser om när och under vilka förutsättningar som brottsbekämpande myndigheter ska få tillgång till de lagrade uppgifterna. Av direktivets artikel 4 följer dock att de nationella bestämmelserna ska försäkra att uppgifter som lagras i enlighet med direktivet endast görs tillgängliga för behöriga nationella myndigheter. Därmed torde denna dörr vara stängd.¹⁸³ I det i avsnitt 4.6 ovan återgivna beslutet av Svea hovrätt (Svea hovrätts beslut ÖÄ 6091-09) berördes som sagt också om datalagringsdirektivet utgör hinder mot att abonnentuppgifter avseende en viss IP-adress över huvud taget lämnas ut till någon annan än en myndighet. I denna fråga fastställde hovrätten utöver vad som redan konstaterats ovan således att datalagringsdirektivet inte heller innebär att sådana uppgifter som inte lagras enligt direktivet är enbart förbehållna behöriga rättsliga myndigheter.¹⁸⁴

Oavsett huruvida en nationell reglering som ger också innehavare av immateriella rättigheter tillgång till uppgifter som lagras enligt datalagringsdirektivet är tillåten enligt gemenskapsrätten, kan problematiken tämligen kort besvaras också utefter vad som föreslås i den svenska utredningen. Där rekommenderas att de uppgifter som tvångsmässigt lagrats i enlighet med datalagringsdirektivet enbart får behandlas av leverantörerna för att lämnas ut efter ett beslut om hemlig teleövervakning eller enligt bestämmelserna i lagen om elektronisk kommunikation (som, vilket också berördes bl.a. i avsnitt 4.2 ovan, är undantag till den tystnadsplikt som gäller för trafikuppgifter och som enbart träffar de uppräknade myndigheterna).¹⁸⁵ I det läckta utkastet till lagrådsremiss sägs att det visserligen är möjligt att införa regler som innebär att trafikuppgifter som lagras också kan lämnas ut för att enskilda ska kunna tillvarata sina rättigheter i en civilrättslig process,¹⁸⁶ men att den svenska lagringsskyldigheten endast ska omfatta brottsbekämpande syften. De nuvarande reglerna i övrigt avses gälla också fortsättningsvis, vilket skulle innebära att de tvångsmässigt lagrade uppgifterna är förbehållna de däri närmare angivna svenska myndigheterna.¹⁸⁷

¹⁸² TT, *Regeringen skjuter sönder Ipred*, Sydsvenskan 2009-05-19.

¹⁸³ Se också SOU 2007:76, s. 182.

¹⁸⁴ Svea hovrätts beslut ÖÄ 6091-09, särskilt sidorna 4 – 5.

¹⁸⁵ SOU 2007:76, s. 181ff. Ett tillägg görs också för fall när annan än leverantören själv ska stå för lagringen av information, för att överföra uppgifterna till denna part.

¹⁸⁶ Jfr. dock föregående stycke. Artikel 4 i direktivet antyder, och Svea hovrätt tillsammans med EG-domstolen i fall C-275/06 anser, att så inte är fallet.

¹⁸⁷ (Läckt utkast till) Lagrådsremiss – Lagring av trafikuppgifter för brottsbekämpning – genomförande av direktiv 2006/24/EG, s. 43ff. Remissutkastet länkas som sagt i internetversionen av Johannisson, *Opublicerad lagrådsremiss om ip-adresser tillbakavisas*, Svenska Dagbladet 2009-05-15.

Med stor sannolikhet kommer därför den (kommande?) svenska implementeringen av datalagringsdirektivet således inte medföra att de uppgifter som ska lagras enligt den nya regleringen också kan begäras ut av rättighetshavare med det immaterialrättsliga informationsföreläggandeinstitutet. Leverantörerna kommer bara att få befatta sig med de tvångsmässigt lagrade uppgifterna för att lämna ut dem efter beslut om hemlig teleövervakning eller enligt bestämmelserna i lagen om elektronisk kommunikation. Rättighetshavares rätt till information kommer således också fortsättningsvis vara avhängigt att informationen fortfarande finns tillgänglig och sparas internt jämte de nuvarande bestämmelserna enligt lagen om elektronisk kommunikation, jfr. avsnitt 6.3 ovan. Skyddet för den tvångsmässigt lagrade informationen i enlighet med direktivet kommer dock inte att ”smitta av sig” eller utökas till den redan sedan tidigare lagrade informationen.

7 Avslutande diskussion

Personlig information är som det framgår på ett flertal ställen i kapitel 2 ovan centralt i de flesta uppfattningar om integritet och former av integritetsproblematik. Med hänsyn till de olika områden som har studerats i denna uppsats kan olika slags integritetsproblematik ses på olika nivåer. Några väldigt intressanta frågor ur integritetssynpunkt är om personlig information över huvud taget bör *lagras*, vilka uppgifter som i så fall bör lagras, samt i vilket syfte. Andra väldigt intressant frågor ur ett integritetsperspektiv är vem som ska få *tillgång* till lagrad personlig information, under vilka förutsättningar, hur den får användas, samt hur missbruk undviks. Dessa frågor är starkt sammanbundna, men samtidigt inte helt förenade.

Den litterära säcken ska i detta kapitel knytas ihop. Uppgiftslagring såsom avses ske enligt datalagringsdirektivet berör på ett första stadium den första gruppen av dessa integritetsfrågor. Kritiken mot direktivet har också riktat sig mot dessa aspekter. Datalagringen berör dock också den andra gruppen av frågor – dessa har huvudsakligen förbisetts i debatten kring uppgiftslagring. Samtidigt utreds dessa frågor i skymundan just nu i polismetodutredningen. Också de två andra regleringar som har undersökts i denna uppsats tangerar dessa viktiga integritetsfrågor. Farhågorna kring och kritiken mot det kommande Telekompaketet har bl.a. rört kontroll och filtrering av information. Implementeringen av Ipred rör huvudsakligen frågor kring tillgång till information. De tre olika områden som studerats i denna uppsats hör således ihop med hänsyn till de integritetsproblem som de aktualiserar. De rör sig visserligen delvis på olika nivåer, men många frågor är gemensamma. Således ska integritetsproblematiken för de områden som studerades i de tre föregående kapitlen i detta uppsatsens sista kapitel diskuteras på dessa nivåer. Eftersom många av integritetsfrågorna är gemensamma, sker därför också diskussionen i ett sammanhang, i ett gemensamt avsnitt.

Ett par ytterligare aspekter med anknytning till integritet ska också diskuteras i detta kapitel. Beträffande Telekompaketet kunde i stort sett samtliga integritetsfarhågor som riktats mot detta, och som samtidigt kan sägas befinna sig på samma nivå som invändningarna mot datalagring och rättighetshavares rätt till information, (tack och lov!) tas död på redan i kapitel 5.¹⁸⁸ Två egendomligheter med den politiska striden och den omkringgårdande debatten kvarstår dock, dessa diskuteras i ett separat avsnitt. Slutligen aktualiserar flagranta fall av integritetsintrång de mänskliga rättigheter som skyddas bl.a. i europakonventionen. Denna problematik utifrån de rättsakter som har studerats i denna uppsats kommenteras kort i ett eget avsnitt.

¹⁸⁸ Se främst avsnitt 5.5 slutet ovan.

7.1 Lagring av personlig information

Ur integritetssynvinkel kritiserades datalagringsdirektivet som berördes i avsnitt 6.4 ovan för den uppgiftslagring som följer av direktivet. Direktivet innebär som sagt att en mängd uppgifter ska lagras under en bestämd tid. Även om den presumtivt kommande svenska regleringen direkt bör ses som ett resultat av Sveriges gemenskapsrättsliga förpliktelser undantar detta inte att innebörden av regleringen bör kunna diskuteras och kritiseras. Datalagring berör som nämndes ovan i första hand den första gruppen intressanta integritetsskyddsfrågor. I detta inledande avsnitt ska således diskuteras om den avsedda informationen över huvud taget bör lagras, och därför bl.a. också sägas något om de syften som har angetts för lagringen och de uppgifter som avses lagras.

Den första frågan i integritetshänseende är naturligtvis om uppgiftslagringen i sig är integritetskränkande, vilket förvisso redan ansetts vara fallet bl.a. av den svenska utredningen.¹⁸⁹ Ett möjligt sätt att angripa denna fråga är att använda William Parents definition av en rätt till personlig integritet.¹⁹⁰ Med denna beskrivning ses integriteten som en rätt till kontroll över information, vilket innebär en rätt till ett tillstånd där odokumenterad personlig information inte är känd eller innehas av andra personer. Uppgiftslagringen enligt datalagringsdirektivet bygger på och förutsätter att personlig information registreras och lagras, därtill i mycket stor omfattning. Redan uppgiftslagringen som sådan kan således ses som en integritetskränkning. Följaktligen behöver inte uppgifterna i ett senare steg också användas eller tas fram för att en kränkning av den personliga integriteten ska inträffa enligt detta synsätt (om än detta naturligtvis inte undantar att detta kan innebära ytterligare integritetskränkningar).¹⁹¹

Nästa, och mer intressanta, fråga blir därefter om denna inskränkning är godtagbar. Av naturliga skäl är det främst här som kritiken mot och debatten kring uppgiftslagringen har legat. Som också berördes främst i kapitel 2 ovan anses rätten till en personlig integritet vanligen inte vara absolut. För att kunna göra en bedömning av när en godtagbar inskränkning av rätten till integritet kan anses vara för handen är det som nämndes i avsnitt 2.3 ovan till stor hjälp om man har några ytterligare värden att väga mot de värden som åberopas till stöd för en inskränkning än att rätten till en personlig integritet enbart har ett etiskt egenvärde. Parent ansåg som bekant att rätten till kontroll över information ska erkännas för att undvika olika former av kränkningar, pga. den skada som ett intrång annars orsakas och upplevs av individen, samt för att de flesta bär på en övertygelse om att inte vilja avslöja vissa uppgifter om sig själva. Utifrån dessa skäl angavs också sex riktlinjer vilka kan tjäna till stöd för att avgöra när och om en godtagbar inskränkning är för handen.

¹⁸⁹ Så är dock inte alltid fallet vad gäller lagstiftaren, jfr. Abrahamsson, s. 424f.

¹⁹⁰ Som ju skildrades i avsnitt 2.7 ovan.

¹⁹¹ Denna del av resonemanget skulle Parent garanterat hålla med om redan 1983. Jfr. avsnitt 2.7 ovan. Se också avsnitt 7.2 nedan.

De skäl som angavs till stöd för uppgiftslagringen enligt direktivet återgavs i avsnitt 6.1 ovan. Dessa var för att underlätta utredning, avslöjande och åtal av allvarligare brottslighet, särskilt organiserad brottslighet. Forskning och praktisk erfarenhet ska också ha visat att sådana uppgifter är särskilt viktiga verktyg för att uppnå dessa syften. Från andra håll har utöver dessa skäl framförts att den svåraste integritetskränkning en individ kan bli utsatt för är ett allvarligt brott, att människor i andra sammanhang frivilligt ger upp stora delar av sin personliga integritet exempelvis genom s.k. sociala medier, samt att personer med rent mjöl i påsen inte behöver bekymra sig om övervakning.¹⁹²

Utifrån Parents sex riktlinjer för att avgöra om en godtagbar inskränkning av rätten till personlig integritet föreligger kan så konstateras att syftet för att den personliga informationen inledningsvis lagras främst är det som återgavs i början av föregående stycke. Nästa fråga, om detta syfte är legitimt och viktigt, är betydligt knepigare att besvara. Implicit i denna fråga ligger också den avvägning som måste göras mellan de olika motstående värdena. Att underlätta utredning, avslöjande och åtal av allvarligare brottslighet bör rimligtvis kunna sägas vara ett legitimt och viktigt syfte.¹⁹³ Det bör dock påpekas att omständigheter som stödjer detta påstående inte har några direkta etiska implikationer.¹⁹⁴

Beträffande de övriga skälen eller argumenten, vilka visserligen inte anförs i ingressen till direktivet men jämväl i debatten, kan följande sägas. Det väldigt vanliga brottsofferargumentet kan visserligen också anses vara legitimt. Det är dock väldigt lätt att missta sig om vad argumentet bygger på – det är ett enskilt allvarligt integritetsintrång som avses. Vid en diskussion som handlar om presumtiva godtagbara inskränkningar av rätten till integritet är med hänsyn till samtyckets centrala funktion i rätten till personlig integritet däremot nästa argument svagt. Rätten till personlig integritet tillerkänner som bekant individen vissa rättigheter, som frivilligt kan efterges. Själva poängen i rättigheten är att individen ges denna kontroll i förhållande till andra individer. Vilka delar av denna rätt många individer i ett senare led väljer att ge upp av en eller annan anledning är i detta hänseende ovidkommande. Argumentet förbiser således ett av de viktigaste momenten i rättighetens utformning, och är därför svagt om det används av någon som i och för sig anser att en rätt till personlig integritet kan sägas vara en skyddsvärd rättighet.¹⁹⁵

¹⁹² Jfr. Abrahamsson, s. 424f, Olsson, ”Rena julafton för kriminella”, Svenska Dagbladet 2009-10-22.

¹⁹³ Om än ett tillägg behöver göras till det anförda skälet (underlättande av utredning osv. av allvarlig brottslighet bör utföras). Märk väl att de effekter som eftersträvas inte är synonyma med att förhindra allvarlig brottslighet. Det går naturligtvis också att ifrågasätta om uppgiftslagring verkligen underlättar utredning m.m. av allvarligare brottslighet, trots försäkranden om saken i ingresstexter.

¹⁹⁴ Jfr. naturalistiskt felsslut, Dahlman, s. 73f. För att detta påstående ska ha det måste preskriptiva premisser läggas till. Se också föregående not.

¹⁹⁵ Jfr. hela kapitel 2 ovan. Ett annat vanligt motargument är att individen vid samtycke frivilligt kan upplåta sin privata sfär för något annat som värdesätts högre.

Därtill innebär inte förhållandet att många väljer att göra en frivillig inskränkning i sin rätt till integritet i något särskilt avseende att denna ”del”, eller dessa personers integritetsskydd över huvud taget, anses vara oviktigt eller oväsentligt av dem själva. Det är dessutom vanligen helt andra slags personliga uppgifter som s.a.s. frivilligt utlämnas än de som omfattas av uppgiftslagringen enligt datalagringsdirektivet. De flesta människor lägger således vanligen inte ut uppgifter rörande vilka IP-nummer de har använt, eller vilka telefonnummer de har ringt eller skickat sms till (tillsammans med tidpunkt och geografisk plats varifrån kommunikationen har skett) på internet, eller sprider eller sparar denna information på något annat sätt. Liknande invändningar som mot detta skäl går att rikta mot det sistnämnda skälet. Rätten till personlig integritet tar i initialläget inte hänsyn till individens presumtiva intentioner. Den gäller för alla. Godtar man rätten till personlig integritet förutsätts således också detta förhållande.¹⁹⁶ Dessa bägge skäl bortses fortsättningsvis från i diskussionen.

För intresseavvägningen mellan underlätandeargumentet och integriteten bör särskilt understrykas vad uppgiftslagringen rent faktiskt innebär. Innebörden i och faktiskt också avsikten med uppgiftslagringen är att *alla individers*, inte bara misstänkta personers, hela elektroniska kommunikationsmönster ska lagras – för att underlätta utredningen, och till och med avslöjandet, av *enskildas* allvarligare brottslighet. Beträffande andra former av straffprocessuella tvångsmedel vilka innebär integritetsintrång och som vanligen inte anses vara lika kontroversiella, som exempelvis hemlig teleavlyssning eller den befintliga möjliga uppgiftsutlämningen enligt lagen om elektronisk kommunikation, bygger dessa på olika grader av *riktade* integritetsintrång, vanligen mot misstänkta gärningsmän eller i alla fall när det finns omständigheter som tyder på brott.¹⁹⁷ Vid den form av uppgiftslagring som nu diskuteras är integritetsintrånget riktat mot alla och envar, och konstant pågående. Underlätandeargumentet på den integritetsnivå vi nu diskuterar medför således också att allas personliga integritet genomgår en konstant begränsning till förmån för presumtiva effektivitetsvinster för brottsutredning. Det kan också påminnas om vad som återgavs i avsnitt 6.4 ovan. Det är väldigt lätt för den som vill att undvika att *användbara* uppgifter för de syften som datalagringen sker vid kommunikation över internet lagras (eller ens är över huvud taget möjliga att lagras). *Då förtas också hela det angivna syftet med uppgiftslagringen, eftersom (användbara) uppgifter enbart för de som med utgångspunkt i lagringssyftet inte är intressanta lagras.*

Det vanliga brottsofferargumentet är faktiskt öppet för samma invändningar. Argumentet används till att motivera omfattande integritetsbegränsningar för *alla* till förmån för att förhindra integritetsintrång eller lidande för *en-*

¹⁹⁶ Uttryckt på ett annat sätt bortser rätten till personlig integritet från mjölfärg. Det är också tråkigt att mjöl ständigt svärtas ned(!) av denna typ av argument.

¹⁹⁷ Den befintliga möjligheten till utlämning av kommunikationsuppgifter bygger som berörts på ett otal ställen på uppgifter som redan finns lagrade av andra skäl. Vid utlämning av dessa uppgifter exv. i brottsutredande syfte sker därmed ett integritetsintrång, som i första hand är riktat. Se också avsnitt 7.2 nedan.

skilda. Brottsofferargumentet förutsätter således att enskildas integritet är på något sätt mer värd än det integritetsintrång som alla drabbas av. Om man ska ta det på allvar förutsätter argumentet dessutom att integritetsintrånget för alla i någon mening *förhindrar* eller *minskar risken för* att mer omfattande integritetsintrång för enskilda inträder. Sammantaget är således brottsofferargumentet egentligen samma argument som underlättandeargumentet men med vissa utbyggnader. Detta innebär också att skenbart olika argument kan anföras till stöd för samma sak.

Beträffande nästa kriterium att ta ställning till kan dock ganska kort konstateras att den kunskap som inhämtas genom integritetsintrånget kan sägas vara relevant för att rättfärdiga detta syfte, eftersom uppgiftslagringen och de därigenom lagrade uppgifterna kan sägas ha en ganska stark koppling åtminstone till de brottsutredande syftena. Som sagt är brottsofferargumentet identiskt med underlättandeargumentet i dessa delar. Nästa fråga, om allomfattande uppgiftslagring är det enda eller minst ingripande sättet att få denna kunskap, är mer intressant. Om inget annat har erfarenheterna med genomförandet av Ipred visat att om en komplett uppgiftslagring eftersträvas är det nödvändigt att kompulsiv lagring införs. Frågan bör dock också ses som om omfattande uppgiftslagring är det enda eller minst ingripande sättet att underlätta utredning, avslöjande och åtal av allvarigare brottslighet.¹⁹⁸ Till och med ett utökat användnings- och tillämpningsområde för befintliga straffprocessuella tvångsmedel torde både totalt sett och för de utsatta individerna vara mindre ingripande ur integritetssynpunkt än den uppgiftslagring som aktualiseras av datalagringsdirektivet. Effektiviteten av ett sådant utökat tillämpningsområde för underlättandet av utredning et cetera torde vara lika (o)säker som den för uppgiftslagring. I vanlig ordning kan också behovet av ett underlättande som sådant ifrågasättas.

De sista riktlinjerna att ta ställning till enligt Parent var slutligen vilka begränsningar och förebyggande åtgärder som fanns i de integritetskränkande förfaranden som man avsåg att använda samt vilket skydd kunskapen får när den väl är inhämtad. Dessa frågor avhandlas i nästa avsnitt. Redan mot uppgiftslagringen som sådan kan det dock redan nu således riktas ett flertal inläggningar.

7.2 Tillgång till personlig information

Den andra gruppen intressanta integritetsskyddsfrågor ifråga om personlig information var som sagt vem som ska få tillgång till lagrad sådan information, under vilka förutsättningar, hur den får användas samt hur missbruk undviks. Datalagringsdirektivet kritiserades huvudsakligen enbart för uppgiftslagringen som sådan, debatten handlade i långt mindre utsträckning om vilka som ska ha rätt att ta del av dessa uppgifter. Dessa frågor reglerades

¹⁹⁸ I omskriven form beträffande brottsofferargumentet, om omfattande uppgiftslagring är det enda sättet att förhindra eller minska risken för enskildas lidande som resultat av att ha blivit utsatta för brott.

som berördes i avsnitt 6.2, 6.3 och 6.5 ovan huvudsakligen inte i direktivet och polismetodutredningen utreder för närvarande bl.a. denna problematik.

Syftet med uppgiftslagringen var som sagt att underlätta bl.a. utredningen av allvarigare brottslighet. För svensk del har enbart brottsutredande myndigheters tillgång till de uppgifter som regelmässigt ska lagras aktualiserats. Frågan om vem som ska ha tillgång till information reser därför inga fler beaktansvärda invändningar ur integritetshänseende beträffande datalagring utöver de som anfördes i föregående avsnitt. Angående under vilka förutsättningar som uppgifterna ska kunna göras tillgängliga har bl.a. framförts farhågor om ändamålsglidning när uppgifterna väl är lagrade.¹⁹⁹ I denna fråga kan i fråga om integritet tilläggas att integritetskränkningar naturligtvis också sker varje gång de lagrade uppgifterna s.a.s. plockas fram och används (se mer utförligt nedan). Och desto lägre krav som upprätthålls för när uppgifterna kan användas, desto mer omfattande blir (den sedan tidigare pågående) integritetskränkningen både totalt sett och mot de individer den särskilt riktar sig mot. En ändamålsglidning kan dessutom sägas ha skett redan om samma förutsättningar som gäller för utlämning av sedan tidigare lagrade uppgifter enligt lagen om elektronisk kommunikation också kommer att gälla för uppgiftsutlämning avseende tvångsmässigt lagrade uppgifter (vilket är fallet enligt utredningsförslaget), eftersom det sammanlagda integritetsintrånget redan genom lagringen är betydligt större.

Begränsningar i hur uppgifterna används samt hur missbruk undviks är som sagt också viktigt ur integritetshänseende. Som nämdes i avsnitt 6.2 och 6.4 ovan har den kraftigt ökade risken vilken är nödvändigt förbunden med att informationsmängden ökar för att informationen läcks, sprids till obehöriga eller används på ett obehörigt framförts från flera olika håll, samtidigt som direktivet överlåter dessa frågor till den nationella regleringen. Den fulla innebörden i dessa frågor bortses dock från i den svenska utredningen, vilket är synnerligen bekymmersamt ur integritetshänseende.

Slutligen beträffande främst datalagringsdirektivet återgavs redan i avsnitt 6.4 ovan att många teleoperatörer var kritiska mot uppgiftslagringen även ur ett kostnadsperspektiv. I denna fråga måste instämmas i vad som också redan anförts – uppgiftslagringen tillför inte verksamheten något mervärde (uppgifterna får som bekant över huvud taget endast användas i de angivna syftena, och bara av brottsbekämpande myndigheter) och kostnaden bör därför åtminstone inte läggas på operatörerna när det som nu verkligen inte rör sig om försumbara kostnader. Uppgiftslagringen som sådan kan också starkt ifrågasättas ur ett rättsekonomiskt perspektiv, särskilt i avseendet de presumtiva brottsutredande vinster som görs i förhållande till de kostnader som staten (inte ens bör utan ska) stå för. Denna omständighet faller dock utanför uppsatsens frågeställning i sin närmare utsträckning.

Också rättighetshavares rätt till information i enlighet med det svenska genomförandet av Ipred aktualiserar ur ett integritetsperspektiv frågor om vem

¹⁹⁹ Också denna fråga omfattas (som sagt) av polismetodens utredning.

som ska få tillgång till lagrad personlig information, under vilka förutsättningar, hur den får användas samt hur missbruk undviks. Som berördes i avsnitt 4.5 ovan var det beträffande implementeringen av Ipred i svensk rätt främst den omfattning som informationsföreläggandeinstitutet kom att få som kritiserades. Ett informationsföreläggande kan som sagt riktas exempelvis mot en internetleverantör som kan föreläggas att lämna ut namnet på den som har haft ett visst IP-nummer vid en enskild tidpunkt varifrån ett misstänkt rättighetsintrång tros ha skett. Lagstiftaren var som berördes i avsnitt 4.2 och 4.4 ovan heller inte, åtminstone på ett principiellt plan, i förhållande till detta direktiv tvungen att innefatta trafikuppgifter från exempelvis internetleverantörer i den rätt till information som ska tillförsäkras rättighetshavare, och problematiken var inte heller i övrigt självklar ens från officiellt håll när regleringen arbetades fram.

Också beträffande genomförandet av Ipred blir den första frågan att ta ställning till om regelverket är integritetskränkande, och i så fall vad som är det.²⁰⁰ Informationsföreläggandeinstitutet förutsätter att personlig information finns lagrad i någon form sedan tidigare hos tjänsteleverantören. Med Parents definition av en rätt till personlig integritet,²⁰¹ kan som fanns vara fallet redan i avsnitt 7.1 ovan bara detta förhållande sägas medföra att utsträckningen av institutet är integritetskränkande. Det är som berördes bl.a. i avsnitt 6.5 ovan dock i någon mening av operatörerna mer ”frivilligt” lagrade uppgifter som kan utlämnas med informationsföreläggandeinstitutet. Utan några större modifikationer av Parents ursprungliga syn på integriteten som en rätt till kontroll över information kan denna dock också sägas tange- ra informationsföreläggandeinstitutets utsträckning genom att personlig information vid användningen av institutet förs vidare till ytterligare personer, därtill vanligen utan individens samtycke eller vetskap. Eftersom rätten till kontroll över information förutsätter (en rätt till) ett tillstånd där personlig information inte är känd eller innehas av andra personer är naturligtvis också redan möjligheten att detta tillstånd inträder, dvs. att personlig information förs över, integritetskränkande enligt detta synsätt.²⁰²

Eftersom förhållandet att rättighetshavare kan få tag på namnet på den som har haft ett visst IP-nummer från en internetleverantör kan ses som en inskränkning av integriteten blir också här nästa naturliga, och mer intressanta, fråga om denna inskränkning är godtagbar. Debatten kring Ipred ligger också huvudsakligen på denna nivå. Också i förhållande till Ipred kan de

²⁰⁰ I detta fall ansåg lagstiftaren åtminstone att en integritetsinskränkning var för handen, genom att redan möjligheten att genom informationsföreläggandeinstitutet få ut personlig information avseende IP-adresser var en inskränkning av integriteten, både på det rättsliga planet som på ett ideellt plan.

²⁰¹ Som skildrades i avsnitt 2.7 och som användes på samma sätt i avsnitt 7.1 ovan.

²⁰² Denna sak skulle Parent däremot 1983 möjligen inte hålla med om, jfr. avsnitt 2.7 ovan. De skäl som angetts av Parent till stöd för hans strikta syn på integritet gör sig emellertid (minst) lika starkt gällande också i den utsträckning som nu diskuteras (särskilt vad gäller de principer som bör tillgodoses ifråga om inskränkningar). Redan i avsnitt 2.7 hänvisades också till Helen Nissenbaums artikel. En bra argumentation till stöd för varför liknande situationer som den som nu diskuteras, och som undantas eller bortses från av vissa äldre synsätt liknande den som förs här görs i hennes artikel.

skäl Parent anförde till stöd för en rätt till personlig integritet samt de riktlinjer vilka kan tjäna till stöd för att avgöra när och om en godtagbar inskränkning är för handen användas.

Det är mot en bakgrund liknande denna som regeringens skäl för regleringens utformning och utsträckning (och i förlängningen till varför en godtagbar inskränkning av integriteten kan anses föreligga) också närmare bör analyseras. Dessa skäl återgavs utförligt i avsnitt 4.4 ovan, men var i korthet följande. Det viktigaste skälet för omfattningen av rättighetshavares rätt till information i det avseende som nu diskuteras var att rättighetshavare enligt svensk rätt före genomförandet av Ipred sällan med rättsliga medel hade möjlighet att på egen hand skaffa sig kunskap om vem som har begått ett misstänkt rättighetsintrång via internet. De enda valmöjligheter rättighetshavare tidigare hade var att be internetleverantörer kontakta sina kunder eller att göra en polisanmälan avseende det misstänkta intrånget. Samtidigt var (och är) intrången via detta medium omfattande, och kunskap om vem som har begått ett intrång var betydelsefull bl.a. för att kunna kontakta intrångsgöraren för att den vägen se till att intrånget kunde upphöra, och att i slutändan kunna tillgripa andra rättsliga medel. Regeringen ansåg att det därför var lämpligt att skapa ett komplement till de straffrättsliga åtgärderna för att öka möjligheterna att ingripa mot intrång genom att ge rättighetshavare en utökad möjlighet att skaffa sådan information som tidigare var förbehållen vissa myndigheter. Regeringen ansåg slutligen att det därför fanns ett starkt intresse för rättighetshavare att få tillgång till personuppgifter kring abonnemangsinnehavare av en IP-adress, och att det integritetsintrång som blev resultatet av att abonnentens identitet röjs var begränsat eftersom den överkomna informationen var betydligt mer begränsad än den som kan åtkommas med befintliga civilprocessrättsliga institut samt att informationen sällan kunde användas till att mer allmänt kartlägga vad enskilda personer gör på internet.

Utifrån Parents sex riktlinjer för att avgöra om en godtagbar inskränkning av rätten till integritet föreligger kan så konstateras att syftet för att den personliga informationen används var att ge rättighetshavare en större möjlighet än den de hade haft tidigare för att ta reda på vem som har begått ett rättighetsintrång – för att i förlängningen på något sätt se till att detta intrång upphör. Beträffande nästa fråga, om detta syfte är legitimt och viktigt, kan sägas att denna fråga också ligger nära huruvida utformningen av den nuvarande immaterialrätten är godtagbar eller bör förändras, en fråga som därtill avsiktligt lämnats utanför denna uppsats. Ett par principiella invändningar mot regeringens motivering ges i slutet av detta avsnitt, vilka definitivt kan sägas äga giltighet också i denna fråga. Åtminstone kan dock sägas att denna problematik försummas i lagstiftarens motivering. Regeringen konstaterade att rättighetshavare har ett starkt intresse av att få tillgång till dessa uppgifter, samtidigt som integritetsintrånget ansågs vara begränsat. Varför detta intresse bör anses vara starkare, mer legitimt eller viktigt motiveras inte mer utförligt.

Framförallt efter integritetsskyddskommitténs slutbetänkande är det att sparka in en öppen dörr att påstå att lagstiftaren gjort (ytterligare) en dålig proportionalitetsavvägning. Att stödja påståendet att integritetsintrånget för abonnenten är begränsat eftersom den utlämnade informationen är mer begränsad än den som kan åtkommas *med andra rättsmedel som finns sedan tidigare* samt att informationen inte går att använda till att göra en allmän kartläggning av vad individen gör är också en tämligen svag form av argumentation när integritetsproblematik diskuteras. En annan sak är att man kan hålla med om lagstiftarens åsikter i sak, men på andra grunder. Under förutsättning att syftet kan sägas böra vara legitimt och viktigt kan dock den personliga information som överlämnas sägas vara relevant för att rättfärdiga detta syfte, eftersom den personliga informationen åtminstone har en stark koppling till detta ändamål.

Om rättighetshavares möjlighet att från internetleverantörer få ut information om innehavare av IP-nummer är det enda eller minst ingripande sättet att ge rättighetshavare en större möjlighet att ingripa mot intrång via internet förbises också i regeringens motivering. Några andra alternativ övervägdes inte. Rättighetshavare hade redan tidigare möjlighet att ingripa mot misstänkta intrång via internet genom en polisanmälan. En annan mindre ingripande lösning för att tillfredsställa det eftersträvade syftet hade t.ex. varit att ge det allmänna bättre resurser och förutsättningar att utreda dessa brott samt att lätta på de legala förutsättningarna för t.ex. polismyndigheten att få ut den information som krävs för att utreda dessa mindre allvarliga brott.

De sista bägge punkter som Parent ansåg att man ska ta ställning till kan anses vara tillfredsställda i något högre grad. Informationen får bara lämnas över efter en rättslig prövning, och sökanden måste visa sannolika skäl för att ett intrång har begåtts. Också när informationen har förts över skyddas den genom bestämmelserna i personuppgiftslagen. Vissa invändningar kan dock resas också mot dessa delar av regleringen. Som berördes i avsnitt 4.5 ovan var en av farhågorna med den föreslagna regleringen att den överlämnade informationen skulle kunna användas otillbörligt i form av "legal utpressning". Skillnaden i styrka och resurser mellan individer och större rättighetshavare, särskilt i form av sammanslutningar och branschorganisationer, ska inte underskattas. Något skydd mot ett sådant förfarande finns inte i den nuvarande regleringen.

Vissa ytterligare principiella invändningar kan slutligen utöver vad som angetts ovan riktas mot regeringens motivering. Som berördes i avsnitt 4.5 har en av de invändningar som riktats mot utformningen av regleringen i debatten varit att en privatisering av delar av brottsbekämpningen kan sägas ha skett. Att dessa invändningar inte kan avfärdas med en axelryckning torde vara uppenbart redan av det som framgått ovan. Redan före implementeringen av Ipred hade rättighetshavare många för immaterialrätten speciella särskilt långtgående rättsmedel till sitt förfogande. Efter genomförandet har dessa möjligheter och befogenheter utökats till att ta reda på vem som har begått ett intrång. Dessa rättigheter sammantagna ger rättighetshavare en inte obetydlig möjlighet att utreda, genomdriva och upprätthålla sina rättig-

heter. Innehavare av immateriella rättigheter har också historiskt i långt högre utsträckning själva fått upprätthålla och genomdriva sina rättigheter jämfört med vad som gäller för vanliga äganderätter, vilka i långt större utsträckning har staten som garant av sitt skydd.²⁰³

Dessa olikheter har naturligtvis motiverats med de skillnader immateriella rättigheter företer i förhållande till fysiska ting. Emellertid ställs många krav på staten när denna agerar exempelvis i egenskap av beskyddare av äganderätten. De bakomliggande skälen till dessa krav bör äga lika stor vikt vad gäller de immateriella rättigheterna. T.ex. återgavs i avsnitt 4.4 ovan att regeringen avfärdade utredningsproblematiken vid anonymisering och öppna privata trådlösa nätverk med att denna var densamma oavsett om ett straff- eller civilrättslig perspektiv antogs. När brottsutredande myndigheter bedriver förundersökning vid misstanke om brott gäller ett flertal rättssäkerhetsprinciper såsom opartiskhets- och objektivitetsprincipen, samt oskyldighetspresumtionen. Ingenting i den svenska regleringen säkerställer att sådana principer direkt upprätthålls vad gäller privata aktörer i egenskap av innehavare av immateriella rättigheter. Det finns också redan nu exempel på fall där sådana principer helt klart verkar ha åsidosatts.²⁰⁴

Även om vissa invändningar således kan riktas mot den svenska omfattningen av rättighetshavares rätt till information är en än viktigare fråga ur integritetshänseende hur långt denna rätt bör sträcka sig i fråga om vilka sorters lagrade uppgifter som kan lämnas ut. Som berördes i avsnitt 6.5 ovan kommer med allra största sannolikhet uppgifter som lagrats i enlighet med datalagringsdirektivet dock inte att kunna lämnas ut till privata aktörer för att stävja immateriella rättighetsintrång.²⁰⁵

7.3 Telekompaketet och tillgång

Om man bara ser till vilka farhågorna har varit och hur debatten har förts kring det kommande Telekompaketet så finns det ett mycket stort antal uppseendeväckande och alarmerande problem som väldigt lätt kan angripas med olika grundläggande rättighets- och integritetsinvändningar, vilka därtill tillhör de bägge nivåer vilka har diskuterats i detta kapitelns bägge föregående avsnitt. I stort sett samtliga av dessa farhågor kunde dock som sagt tas död på redan i kapitel 5.²⁰⁶ Eftersom dessa problem i vissa fall aldrig, och för de flesta övriga fall åtminstone inte längre, kommer att aktualiseras finns det ingen anledning till att uppmärksamma eller diskutera dessa ytterligare. Den huvudsakliga politiska striden vid antagandet av det nya Telekompake-

²⁰³ Det ska naturligtvis särskilt understrykas att immateriella rättigheter *inte* har mer gemensamt med äganderätten än med exempelvis arrende eller lån.

²⁰⁴ Jfr. Svea hovrätts beslut ÖA 6091-09. Som berördes i avsnitt 4.6 ovan saknades utredning i många – väsentliga – delar. Misstankarna om dataintrång med den svenska utformningen av detta brott kan minst sagt sägas vara grundade. Det behöver knappast heller påminnas om hur svensk rätt ser på brottsprovokationer när dessa utförs av polisen.

²⁰⁵ Jfr. dock ovan gällande ändamålsglidning.

²⁰⁶ Se särskilt sista styckena i avsnitt 5.5

tet låg som bekant i huruvida ett krav på att en föregående domstolsprövning måste ske vid exempelvis en begränsning av en användares internettillgång skulle införas i direktivtexten eller inte. Denna fråga var också den mest uppmärksammade i den omkringgårdande debatten. Det är två saker som är egendomliga med detta förhållande, och det är dessa som ska behandlas i detta avsnitt. Den i och för sig väldigt intressanta frågan kring tjänsteleverantörers och nätoperatörers framtida roll bortses således från i detta avsnitt. Denna fråga ligger dessutom ganska långt bort från en integritetsdiskussion.

Den första konstigheten med det nya Telekompaketet och den politiska striden kring det, handlar om den fråga som från början var innehållet i Europaparlamentets ändringsförslag 138. Som bekant innehöll detta ändringsförslag ett krav på att en rättslig prövning ska ske före påförandet av en statligt upprätthållen sanktion innebärande att restriktioner införs i slutanvändarnas grundläggande friheter, som t.ex. en begränsning av en användares tillgång till internet. Ett sådant krav kan med allra största säkerhet redan sägas gälla för samtliga europeiska länder som har tillträtt europakonventionen.²⁰⁷ (Och som av en slump är alla medlemsstater i EG/EU bundna konventionen.) Att en bestämmelse som erinrar om detta faktum möjligen är något malplacerad i ett direktiv som i övrigt reglerar infrastruktur är sedan en helt annan fråga. Med hänsyn till att ett krav på rättslig prövning obestridbart redan gäller är det dock uppseendeväckande att denna fråga, som i det närmaste således bara är estetisk,²⁰⁸ nära nog förhindrade att rättsakterna kunde antas. Att sedan det som regleras i kompromissen också redan borde gälla enligt europakonventionen och därför kan anses vara onödigt må så vara. Kompromissen torde vara lika (o)förenlig med artikel 95 EGF som ändringsförslag 138 av samma anledning. Att det franska nationella författningsförslaget om dylika sanktioner såsom det ursprungligen utformats fick arbetas om är däremot inte alls sensationellt.

Den största egendomligheten med den politiska striden (men också den omkringgårdande debatten) är dock att den de facto rört denna fråga – den ”presumptiva” rätten till föregående domstolsprövning vid påförandet av ifrågavarande restriktioner – och inte sanktionerna i sig. Rimligheten och proportionaliteten i att ålägga en restriktion som går ut på att t.ex. avsluta en individs tillgång till internet som en reaktion på ett, i vissa fall t.o.m. miss-tänkt, immaterialrättsintrång (eller ens över huvud taget) har inte alls be-lysts, eller i bästa fall hamnat i skymundan. Denna fråga kan ses såväl på ett moraliskt som på ett rättsligt plan.

På det ideella planet kan frågan naturligtvis ses ur ett integritetsperspektiv, men också ett yttrandefrihetsperspektiv ligger väldigt nära till hands.²⁰⁹ Vil-

²⁰⁷ Detta är så självklart att jag inte ens tänker ange någon källa. De läsare vilka också råkar vara gemenskapsrättsliga politiker och/eller nationella makthavare och inte känner till detta bör genast läsa artikel 6 EKMR på lämpligt språk.

²⁰⁸ Jfr. avsnitt 5.4 ovan ang. rådets skäl.

²⁰⁹ Det finns inte utrymme för en utveckling också av yttrandefrihetsteori i denna uppsats. Rättigheterna har dock många liknande rötter och drag, och inte heller yttrandefriheten

ket perspektiv man än antar är dock sådana former av sanktioner tämligen enkla att rikta invändningar mot. Med just internet och immaterialrättsintrång som exempel kan det konstateras att internet vanligen används i några fler syften än illegal fildelning, samordning av brottslighet, terroristverksamhet, sexuella ändamål eller annan dekadent, klandervärd, skadlig och/eller förkastlig verksamhet. Naturligtvis är det ingen individ som skulle få betydande fysiska eller psykiska skador av att tvingas vara utan internet-tillgång i dagens samhälle (eller åtminstone ett väldigt litet antal). Ett normalt fungerande samhällsliv blir dock kraftigt kringskuret när stora delar av möjligheterna till för många människor idag normal och daglig kommunikation starkt försvåras eller omöjliggörs. De sanktioner som idag används som reaktion på icke önskvärda handlingar begränsar sig till frihetsstraff och ekonomiska sanktioner. Inskränkningar av möjligheten att uttrycka sig och kommunicera som en rättsligt påförd sanktion eller påföljd har inte funnits i Sverige eller stora delar av Europa sedan andra världskrigets slut.

Vad gäller särskilt immateriella rättigheter hör dessa huvudsakligen till civilrättens område, även om ett litet straffrättsligt inslag också finns. Intrång i immateriella rättigheter orsakar ideella skador, och i vissa fall också förmögenhetsskador. Skadorna orsakas rättigheternas innehavare. Visserligen är en avstängning av internetanslutning ett obestridbart effektivt sätt att avvärja fildelning från det ifrågavarande abonnemanget eftersom det bygger på inkapacitering (och möjligen också omedelbar avskräckning). Som sanktion för de typer av skador och skadelidande som nu avses är dessa former av begränsningar emellertid inte bara disproportionerliga utan drakoniska. Gärningens förkastlighet och den orsakade skadan kan över huvud taget inte sägas stå i proportion till den skada som genom sanktionen vållas gärningsmannen. Presumtivt åsyftade preventiva eller medelbart avskräckande effekter är inte klarlagda (och troligtvis inte ens påtänkta), och de idag befintliga immaterialrättsliga sanktionerna är betydligt mindre ingripande.

Också vad som ursprungligen reglerades i Europaparlamentets ändringsförslag 166,²¹⁰ att restriktioner som införs för användares rätt till tillgång till bl.a. innehåll sker i enlighet med principerna om proportionalitet, effektivitet och avskräckning, borde gälla redan enligt europakonventionen, särskilt artiklarna 8 och 10.²¹¹ Det är något oklart om ändringsförslag 166 var avsiktligt riktat mot sådana begränsningar liknande de som diskuterades i föregående stycken. I vilket fall måste de vara förenliga med europakonventionen, men det kan sägas vara oklart att de definitivt är det. För att begränsningarna ska vara så måste de enligt både artikel 8 och 10 ske med stöd i lag, tillgodose ett enskilt eller allmänt intresse samt vara nödvändiga i ett demokratiskt samhälle. Ett av de godtagbara intressena enligt både artikel 8

brukar anses vara absolut. Det kan också tilläggas att det eg. torde vara rättigheten med rötter i rätten till personlig integritet och yttrandefrihet med det engelska namnet "freedom of information" som moralfilosofiskt ligger närmast detta problemområde.

²¹⁰ Se avsnitt 5.4 ovan.

²¹¹ Jfr. avsnitt 3.4 ovan. Också artikel 10 är möjlig att inskränka under liknande förutsättningar som artikel 8, och dessa förutsättningar är väldigt lika de som återges i ändringsförslag 166.

och artikel 10 är skyddet av andra personers fri- och rättigheter, vartill bl.a. äganderätten och immaterialrätten brukar räknas. Det tveksamma ligger i om en sådan begränsning kan anses vara godtagbar i ett demokratiskt samhälle i europakonventionens mening. Sanktionerna är som sagt på väg att införas i Frankrike, och Storbritannien har också visat ett visst intresse för liknande sanktioner. Framtiden lär få utvisa vad som gäller i detta avseende.

Slutligen kan ett par rent allmänna problem också anges för restriktioner av användares grundläggande friheter som t.ex. internettillgång. Den franska nationella regleringen innebär att abonnentens internetabonnemang avslutas samt att abonnenten hindras från att teckna ett nytt avtal med sin nuvarande leverantör eller med andra. Detta medför emellertid inte att abonnentens möjlighet till rättighetsintrång via internet helt omöjliggörs. Möjligheterna att få tillgång till internet utan ett internetabonnemang för den som verkligen vill på mer eller mindre legala vägar är stora idag, bl.a. på arbetsplatsen, genom avsiktligt eller oavsiktligt öppna privata eller kommersiella trådlösa nätverk, eller via mobiltelefoninätet med ett anonymt kontantkort. Om en fullständig avstängning från internet eftersträvas måste dessa vägar på något sätt hejdas. Dessutom går i stort sett alla former av elektronisk kommunikation idag via internet någonstans på vägen, inklusive vanlig telefoni. Om också dessa former av kommunikation ska hindras väger argumenten som har återgetts ovan ännu tyngre.

7.4 Europakonventionen revisited

Såväl den datalagring som avses ske enligt datalagringsdirektivet som Telekompaketet och det svenska genomförandet av Ipred har som berörts på ett flertal ställen tidigare i uppsatsen också kritiserats såsom stridande mot de rättigheter som ges i europakonventionen. Beträffande Telekompaketet berördes delar av denna problematik i avsnitt 7.3 här ovan (några större faror kunde som bekant åtminstone inte sägas återstå). I detta avsnitt ska sägas något ytterligare om just datalagring och det svenska genomförandet av Ipred i förhållande till europakonventionen, framförallt dess artikel 8.²¹²

Beträffande den svenska implementeringen av Ipred och omfattningen av rättighetshavares rätt till information ifrågasatte som berördes i avsnitt 4.4 ovan bl.a. någon remissinstans om denna var i överensstämmelse med europakonventionen. Denna fråga är dock troligtvis ganska enkel att besvara. Europadomstolen har visserligen varken direkt prövat direktivet på detta sätt eller det svenska genomförandet. Men med hänvisning till EG-domstolens uttalanden i domen C-275/06 är det mycket avlägset att direktivet skulle vara konventionsstridigt.²¹³ Den av regeringen för det svenska genomförandet utförda proportionalitetsavvägningen går visserligen att kritisera,²¹⁴ men vid en prövning i Europadomstolen skulle domstolen i vilket fall göra en

²¹² Vilken kort behandlades i avsnitt 3.4 ovan.

²¹³ Se särskilt p. 63 och framåt i C-275/06.

²¹⁴ Se avsnitt 7.2 ovan.

egen avvägning. Europadomstolen är naturligtvis inte bunden av EG-domstolens avgöranden, men det finns inga tecken på något som skulle kunna motivera en annan utgång i Europadomstolen heller vad gäller den svenska implementeringen.²¹⁵

Vad gäller datalagringsdirektivet har åtminstone nationellt fler röster höjts om detta direktivs (o)förenlighet med europakonventionen.²¹⁶ Detta direktiv har emellertid inte prövats vare sig av Europadomstolen eller av EG-domstolen i detta avseende. Utöver att konstatera att uppgiftslagringen faller inom tillämpningsområdet för främst artikel 8 i konventionen skulle ytterligare uttalanden i denna fråga inte vara annat än (möjligen i och för sig kvalificerade) gissningar. Som med önskad klarhet har framgått främst av avsnitt 7.1 och 7.2 ovan kan uppgiftslagringen åtminstone ifrågasättas på ett ideellt plan. EG-domstolen underströk därtill visserligen som nämndes i avsnitt 6.4 ovan när den rättsliga grunden för datalagringsdirektivet prövades att det inte påstås i målet att direktivet skulle innebära ett eventuellt åsidosättande av grundläggande rättigheter. Det är dock direkt olämpligt att dra några mer långtgående slutsatser av ett sådant uttalande.

²¹⁵ Jfr. C-275/06, särskilt p. 63 och framåt.

²¹⁶ Se bl.a. avsnitt 6.4 ovan.

Slutligen kan nämnas att den rumänska(!) författningsdomstolen i oktober 2009 prövade den rumänska implementeringen av datalagringsdirektivets överensstämmelse med den rumänska konstitutionen och europakonventionen. Den rumänska författningsdomstolen förklarade kontinuerlig generell datalagring vara i sig oförenlig med den rumänska konstitutionen och *euro-pakonventionen*. Domen har också översatts till engelska, och säger således bl.a. i ett avsnitt;²¹⁷

The Constitutional Court underlines that the justified use, under the conditions regulated by law 298/2008 [den nationella lagen, min anm.], is not the one that in itself harms in an unacceptable way the exercise of the right to privacy or the freedom of expression, *but rather the legal obligation with a continuous character, generally applicable, of data retention*.* This operation equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform *a priori* all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes. *Law 298/2008*,* even though it uses notions and procedures specific to the penal law, *has a large applicability** – practically to all physical and legal persons users of electronic communication services or public communication networks – *so, it can't be considered to be in agreement with the provisions in the Constitution and Convention for the defence of human rights and fundamental freedoms regarding the guaranteeing of the rights to private life, secrecy of the correspondence and freedom of expression*.*

* [mina kursiveringar]

Naturligtvis har avgöranden från Rumäniens författningsdomstol ett än mindre rättskällevärde i Europadomstolen än avgöranden från EG-domstolen. Men resonemangen är intressanta, och visar åtminstone att uppgiftslagring på ett seriöst vis kan ifrågasättas också rättsligt. Man kan bara hoppas att Europadomstolen och/eller EG-domstolen i framtiden blir tvungna att ta ställning i denna fråga.

²¹⁷ Domen bör läsas i sin helhet, men bara ett kortare avsnitt kan av utrymmesskal återges här (om än den är på endast 11 sidor). Den engelska översättningen för de vars rumänska är något ringrostig finns tillgänglig på <http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html> (2009-12-05), samt i pdf-format på http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (2009-12-18).

7.5 Integritetsproblematiken i framtiden

De sista rader som nu nedtecknas i denna uppsats sammanfaller med de sista rader som jag kommer att skriva under mina nio terminer vid juristutbildningen. Beträffande framtiden är som bekant bara två saker säkra; skatter och döden.²¹⁸ I denna uppsats har enbart förhållanden fram till dags dato behandlats. Något bör avslutningsvis också sägas inför framtiden.

De senaste decenniernas tekniska utveckling, som också kan väntas fortsätta inom den närmsta överskådliga framtiden, har fört med sig aldrig tidigare skådade möjligheter för såväl privata som offentliga organ att övervaka och kartlägga människors privata förehavanden. Rätten till en personlig integritet ansågs i integritetsskyddskommitténs slutbetänkande ha utsatts för särskilt många inskränkningar de senaste åren, och lagstiftaren kan med skäl kritiseras för att ha saknat en helhetssyn för integritetsskyddsaspekter vid de senaste årens rättsliga utveckling inom de områden där den personliga integriteten särskilt berörs.²¹⁹

I integritetsskyddsfrågor kan över huvud taget konstateras att uppfattningen om vad integritet är, vad som skyddas, samt vilka inskränkningar av den som är godtagbara, förändras över tiden. Många frågor som var kontroversiella igår, är idag allmänt accepterade. Och många frågor som är kontroversiella idag, kan imorgon komma att framstå som obefogade. Det är i detta sammanhang dock viktigt att komma ihåg att detta förhållande naturligtvis inte följer med nödvändighet. Alla de frågor som var kontroversiella ur ett integritetsperspektiv under 70-talet är inte accepterade idag, och allt som är kontroversiellt idag kommer inte att vara accepterat imorgon. Utvecklingen kan också gå i motsatt riktning.

Med detta sagt kan några mer specifika exempel nämnas, varav det första av dem har en typisk kuriosaprägel. Idag torde polisens rätt att ta till och med rutinmässiga alkoholutandningsprov ha en kraftigt utbredd acceptans i samhället. Men när polisen skulle ges tillåtelse att använda denna metod under 70-talet fanns det på regeringskansliet farhågor om att bilförare skulle uppleva dessa prov som integritetskränkande och ha effekten att bilförare upplever att de lever (kör?) i ett övervakningssamhälle. Denna oro ska särskilt ha uttryckts bl.a. av finansminister Gunnar Sträng(!).²²⁰ Ett mer närliggande exempel, och en bra poäng, är att tyngdpunkten såväl nationellt som på gemenskapsnivå när mobiltelefonin och samtida andra mer sofistikerade digitala kommunikationsnät än det vanliga analoga telefonnätet började växa fram för inte särskilt många år sedan låg på att *hindra* tjänsteleverantörer från att lagra trafikuppgifter och annan personlig information om användar-

²¹⁸ I den gamla harangen eller tiraden brukar ju också tillägget ”beträffande den sistnämnda är jag inte helt säker” göras.

²¹⁹ Jfr. Abrahamsson, s. 427f. Att den däri förespråkade lösningen sedan vid närmare eftertanke kanske inte är den bästa må så vara, jfr. Munck, s. 499ff.

²²⁰ Munck, s. 503. Naturligtvis måste Johan Munck särskilt tackas för återgivandet av denna förträffliga anekdot.

na. Uppgifterna skulle utplånas eller avidentifieras så fort samtalet var avslutat, och undantag gjordes i ett fåtal praktiska fall såsom för fakturahantering. Farhågor fanns bl.a. för att känsliga uppgifter skulle komma att användas i otillbörliga syften eller hamna i orätta händer. Nu, bara några år senare, införs istället en *lagringsskyldighet* för tjänsteleverantörer för samma slags uppgifter avseende samma typer av känslig personlig information, varken för tjänsteleverantörernas eller kundernas skull, utan för staten och brottsbekämpningen.²²¹

En liknande bra poäng gäller förhållandet att myndigheter, banker och butikskedjor idag lagrar uppgifter om våra telefonsamtal, ekonomiska transaktioner och köpvanor. Genom kund- och rabattsystem fås tillgång till uppgifter som endast mycket sofistikerade marknadsundersökningar annars skulle kunna ge, och som också måste kunna anses ha ett stort ekonomiskt värde. Att de flesta idag inte heller behöver deklarerera eftersom i detta fall skatteverket vanligen redan har alla uppgifter som krävs för att räkna ut skatten till sitt förfogande är ett annat sådant förhållande som idag aldrig, eller åtminstone ytterst sällan, ifrågasätts.²²²

Vad finns det då att lära av detta? Det senaste decenniets trend med utökade befogenheter bl.a. för brottsutredande organ och i säkerhetspolitiska syften (vilken i många sammanhang också har beskrivits ha fått sin början med händelserna i New York den 11 september 2001) med därtill nödvändigt förbundna integritetsinskränkningar har om inget annat gjort integriteten till en av vår tids viktigaste rättspolitiska frågor.²²³

Inför framtiden kan således följande sägas.

De frågor som behandlas i denna uppsats var väldigt viktiga, omdebatterade och i några fall också synnerligen politiskt kontroversiella vid den tidpunkt uppsatsen skrevs.

Vi befinner oss idag fortfarande relativt långt från ett dystopiskt övervakningssamhälle.

Samtidigt är det uppenbarligen väldigt lätt att förblindas av effektivitetsskäl och säkerhetsvinster när en avvägning ska göras mot andra ”mjukare”, mer ”svårgreppbara” och ”diffusa” värden som ”integritet”.

Om dessa ”diffusa” värden tillåts att stå i skymundan i framtiden, kommer stora delar av dagens rättighetsuppfattningar komma att behöva förändras i grunden.

²²¹ Axberger, s. 478f.

²²² Axberger, s. 480.

²²³ Jfr. Munck, s. 501.

Käll- och litteraturförteckning

Artiklar

- Abrahamsson, Olle, *Integritetsskydd med eller utan förnuft*, i Svensk Juristtidning 2009, s. 421 – 434, *cit. Abrahamsson*.
- Axberger, Hans-Gunnar, *Integritetsskydd i perspektiv*, i Svensk Juristtidning 2009, s. 468 – 482, *cit. Axberger*.
- Bloustein, Edward J., *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, i New York University Law Review 1964, s. 962 – 1007, *cit. Bloustein*.
- Gavison, Ruth, *Privacy and the Limits of Law*, The Yale Law Journal 1980, s. 421 – 471, *cit. Gavison*.
- Gerstein, Robert S., *Intimacy and Privacy*, Ethics 1978, s. 76 – 81, *cit. Gerstein*.
- Hallborg, Jr., Robert B., *Principles of Liberty and the Right to Privacy*, i Law and Philosophy 1986, s. 175 – 218, *cit. Hallborg, Jr.*
- Klamberg, Mark, *FRA:s signalspaning ur ett rättsligt perspektiv*, i Svensk Juristtidning 2009, s. 519 – 541.
- Lännergren, Bengt, *Om integritet*, i Svensk Juristtidning 1979, s. 161 – 181, *cit. Lännergren*.
- Moore, Adam, *Defining Privacy*, i Journal of Social Philosophy 2008, s. 411 – 428, *cit. Moore 2008*.
- Moore, Adam, *Privacy: Its Meaning and Value*, i American Philosophical Quarterly 2003, s. 215 – 227, *cit. Moore 2003*.
- Munck, Johan, *Synpunkter på några integritetsskyddsfrågor*, i Svensk Juristtidning 2009, s. 499 – 505, *cit. Munck*.
- Nissenbaum, Helen, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, i Law and Philosophy 1998, s. 559 – 596, *cit. Nissenbaum*.
- Parent, William A., *A New Definition of Privacy for the Law*, i Law and Philosophy 1983, s. 305 – 338, *cit. Parent 1983b*.

Parent, William A., *Privacy, Morality, and the Law*, i Philosophy and Public Affairs 1983, s. 269 – 288, *cit. Parent 1983a*.

Rachels, James, *Why Privacy is Important*, i Philosophy and Public Affairs 1975, s. 323 – 333, *cit. Rachels*.

Reimers, Elisabet, *Integritetsskyddet i regeringsformen*, i Svensk Juristtidning 2009, s. 435 – 451, *cit. Reimers*.

Scanlon, Thomas, *Thomson on Privacy*, i Philosophy and Public Affairs 1975, s. 315 – 322, *cit. Scanlon*.

Thomson, Judith Jarvis, *The Right to Privacy*, i Philosophy and Public Affairs 1975, s. 295 – 314, *cit. Thomson*.

Warren, Samuel D., Brandeis, Louis D., *The Right to Privacy*, i Harvard Law Review 1890, s. 193 – 220, *cit. Warren & Brandeis*.

Litteratur

Dahlman, Christian, *Rätt och rättfärdigande – En tematisk introduktion i allmän rättslära*, Studentlitteratur, Polen 2007, *cit. Dahlman*.

DeCew, Judith, Zalta, Edward N. (red.), *Privacy*, The Stanford Encyclopedia of Philosophy, Fall 2008 Edition, <http://plato.stanford.edu/archives/fall2008/entries/privacy/>, *cit. DeCew*.

Locke, John, *Two Treatises of Government – Edited with an Introduction and Notes by Peter Laslett*, Student edition, Cambridge University Press, Cambridge 1999, *cit. Locke*.

Mill, John Stuart, *On Liberty and other essays – Edited with an Introduction and Notes by John Gray*, Oxford University Press, St Ives 1998, *cit. Mill*.

Wolff, Jonathan, *An Introduction to Political Philosophy revised edition*, Oxford University Press, Great Britain 2006, *cit. Wolff*.

Offentligt tryck

Lagrådsremiss – Lagring av trafikuppgifter för brottsbekämpning – genomförande av direktiv 2006/24/EG. Se Johannisson, *Opublicerad lagrådsremiss om ip-adresser tillbakavisas*, Svenska Dagbladet 2009-05-15 nedan för länkadress.

Prop. 1975/76:209. Ändring i regeringsformen.

Prop. 1987/88:57. Grundlagsfäst integritetsskydd.

Prop. 1993/94:117. Inkorporering av Europakonventionen och andra fri- och rättighetsfrågor.

Prop. 1997/98:44. Personuppgiftslag.

Prop. 2001/02:72. Ändringar i regeringsformen – samarbetet i EU m.m.

Prop. 2002/03:110. Lag om elektronisk kommunikation, m.m.

Prop. 2008/09:67. Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG.

Regeringskansliet faktapromemoria 2007/08:FPM45. EU:s översyn av Regelverket för elektroniska kommunikationer.

SOU 1984:54. Tvångsmedel – Anonymitet – Integritet. Betänkande av tvångsmedelskommittén.

SOU 1987:74. Optisk-elektronisk övervakning. Betänkande av utredningen om TV-övervakning m.m.

SOU 2007:76. Lagring av trafikuppgifter för brottsbekämpning. Betänkande av Trafikuppgiftsutredningen.

SOU 2008:3. Skyddet för den personliga integriteten – bedömningar och förslag.

SOU 2008:125. En reformerad grundlag. Betänkande. Del 1 och 2 av Grundlagsutredningen.

Rättsakter från unionen

A6-0272/2009. Andrabehandlingsrekommendation.

A6-0257/2009. Andrabehandlingsrekommendation.

KOM(2007) 697. Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv 2002/21/EG om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/19/EG om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter och direktiv 2002/20/EG om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster.

KOM(2007) 698. Förslag till Europaparlamentets och rådets direktiv om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om konsumentskyddssamarbete.

KOM(2007) 699. Förslag till Europaparlamentets och rådets förordning om inrättande av en europeisk myndighet för marknaden för elektronisk kommunikation.

KOM(2008) 723. Ändrat förslag till Europaparlamentets och rådets direktiv om ändring av direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och förordning (EG) nr 2006/2004 om konsumentskyddssamarbete.

KOM(2008) 724. Ändrat förslag till Europaparlamentets och rådets direktiv om ändring av direktiv 2002/21/EG om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, direktiv 2002/19/EG om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter och direktiv 2002/20/EG om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster.

KOM(2009) 420. Kommissionens yttrande.

KOM(2009) 421. Kommissionens yttrande.

P6_TA(2008)0449. Europaparlamentets lagstiftningsresolution.

P6_TA(2008)0452. Europaparlamentets lagstiftningsresolution.

P6_TA(2009)0360. Europaparlamentets lagstiftningsresolution.

P6_TA(2009)0361. Europaparlamentets lagstiftningsresolution.

P6_TC1-COD(2007)0247. Europaparlamentets ståndpunkt.

P6_TC1-COD(2007)0248. Europaparlamentets ståndpunkt.

P6_TC2-COD(2007)0247. Europaparlamentets ståndpunkt.

P6_TC2-COD(2007)0248. Europaparlamentets ståndpunkt.

P7_TA-PROV(2009)0068. Europaparlamentets lagstiftningsresolution.

PE-CONS 3677/09. Gemensamt utkast godkänt av förlikningskommittén.

PE420.223. Förslag till andrabehandlings-rekommendation.

PE421.119. Förslag till andrabehandlings-rekommendation.

PE430.561v02-00. Betänkande om förlikningskommitténs gemensamma utkast.

Rådets gemensamma ståndpunkt 16496/1/08.

Rådets gemensamma ståndpunkt 16497/1/08.

Tidningsartiklar

Brandel, Tobias, *Piratpartiet EU-valets stora segrare*, Svenska Dagbladet 2009-06-08. (http://www.svd.se/nyheter/politik/euvalet2009/piratpartiet-eu-valets-stora-segrare_3027885.svd 2009-12-18.)

Brinkhäll, Patrik, *Så enkelt lurar du FRA*, i Datormagazin nummer 3 2009, s. 36 – 39.

Carp, Ossi, *IT-branschen: ”Telekompaketet behöver tillägg om mänskliga rättigheter”*, Dagens Nyheter 2009-05-05. (<http://www.dn.se/kultur-noje/film-tv/it-branschen-telekompaketet-behoover-tillagg-om-manskliga-rattigheter-1.858416> 2009-12-18.)

Fransson, Anne-Marie, Franzen, Tomas, Heilborn, Erik, Ganev, Georgi, Karlung, Jon, Ek, Mikael, Palmstierna, Niclas, Norberg, Ola, Söderberg, Roger, & Trampus, Stefan, *Nätoperatörernas roll görs omöjlig*, Svenska Dagbladet Brännpunkt 2009-09-30. (http://www.svd.se/opinion/brannpunkt/natoperatorernas-roll-gors-omojlig_3584645.svd 2009-12-18.)

- Goldberg, Daniel, *Internettrafiken dyker*, IDG.se 2009-04-01.
(<http://it24.idg.se/2.2275/1.221785/internettrafiken-dyker> 2009-12-18.)
- Gustafsson, Sten, "*Fildelarlagen farligare än FRA-lagen*", Dagens Nyheter 2008-11-29. (<http://www.dn.se/nyheter/sverige/fildelarlagen-farligare-an-fra-lagen-1.470008> 2009-12-18.)
- Hammarqvist, Johan, *Alliansens svek mot den personliga integriteten*, Norra Skåne 2009-02-24. (<http://www.nsk.se/article/20090224/OPINION/257800591> 2009-12-18.)
- Johannisson, Emma, *Opublicerad lagrådsremiss om ip-adresser tillbakavisas*, Svenska Dagbladet 2009-05-15. (http://www.svd.se/nyheter/inrikes/opublicerad-lagratsremiss-om-ip-adresser-tillbakavisas_2902057.svd 2009-12-18.)
- Lewan, Mats, *Internettrafiken halverades igår*, Ny Teknik 2009-04-02.
(http://www.nyteknik.se/nyheter/it_telekom/internet/article550628.ece 2009-12-18.)
- Mesta motståndets lag*, Huvudledare Sydsvenskan 2009-03-18.
(<http://sydsvenskan.se/opinion/huvudledare/article420308/Mesta-motstandets-lag.html> 2009-12-18.)
- Nilsson, David Nannini, *Artister stödjer "IPRED-lagen"*, Aftonbladet 2008-11-13. (<http://www.aftonbladet.se/nyheter/ipred/article3758210.ab> 2009-12-18.)
- Nilsson, Owe, *Tele 2 raderar Ipreduppgifter*, Svenska Dagbladet 2009-04-28. (http://www.svd.se/nyheter/inrikes/tele-2-raderar-ipreduppgifter_2804863.svd 2009-12-18.)
- Olsson, Tobias, "*Rena julafton för kriminella*", Svenska Dagbladet 2009-10-22. (http://www.svd.se/nyheter/inrikes/rena-julafton-for-kriminella_3691035.svd 2009-12-18.)
- Olsson, Tobias, "*Sverige bryter mot de mänskliga rättigheterna*", Svenska Dagbladet 2009-02-11. (http://www.svd.se/nyheter/inrikes/sverige-bryter-mot-de-manskliga-rattigheterna_2455045.svd 2009-12-18.)
- Olsson, Tobias, *Bakslag för internetaktivister om telekompaketet*, Svenska Dagbladet 2009-09-28. (http://www.svd.se/nyheter/inrikes/bakslag-for-internetaktivister-om-telekompaketet_3580273.svd 2009-12-18.)
- Olsson, Tobias, *Brott mot svensk grundlag?*, Svenska Dagbladet 2008-12-12. (http://www.svd.se/nyheter/politik/brott-mot-svensk-grundlag_2189089.svd 2009-12-18.)

Olsson, Tobias, *Datalagring får tyskar att sluta ringa*, Svenska Dagbladet 2008-12-17. (http://www.svd.se/nyheter/politik/datalagring-far-tyskar-att-sluta-ringa_2214133.svd 2009-12-18.)

Olsson, Tobias, *Datalagring kan kosta 1 miljard*, Svenska Dagbladet 2008-12-12. (http://www.svd.se/nyheter/inrikes/datalagring-kan-kosta-1-miljard_2194989.svd 2009-12-18.)

Olsson, Tobias, *Grönt ljus för datalagring*, Svenska Dagbladet 2009-02-10. (http://www.svd.se/nyheter/inrikes/gront-ljus-for-datalagring_2450033.svd 2009-12-18.)

Olsson, Tobias, *Ingen datalagring före sommaren*, Svenska Dagbladet 2009-06-12. (http://www.svd.se/nyheter/politik/ingen-datalagring-fore-sommaren_3047885.svd 2009-12-18.)

Olsson, Tobias, *Klart nej till ny fildelningslag*, Svenska Dagbladet 2009-03-17. (http://www.svd.se/nyheter/inrikes/klart-nej-till-ny-fildelningslag_2604781.svd 2009-12-18.)

Olsson, Tobias, *Ny fildelningslag skapar nätuppror*, Svenska Dagbladet 2008-11-12. (http://www.svd.se/nyheter/inrikes/artikel_2028533.svd 2009-12-18.)

Olsson, Tobias, *Sverige stäms för datalagring*, Svenska Dagbladet 2009-05-26. (http://www.svd.se/nyheter/inrikes/sverige-stams-for-datalagring_2954845.svd 2009-12-18.)

Olsson, Tobias, *Telekompaketet ska öka konsumenternas rättigheter*, Svenska Dagbladet 2009-05-04. (http://www.svd.se/nyheter/politik/euvalet2009/telekompaketet-ska-oka-konsumenternas-rattigheter_2835267.svd 2009-12-18.)

Phillips, Leigh, *France Passes Tough Internet Piracy Bill*, BusinessWeek 2009-09-17. (http://www.businessweek.com/globalbiz/content/sep2009/gb20090917_225687.htm 2009-12-18.)

Pfanner, Eric, *France Approves Wide Crackdown on Net Piracy*, The New York Times 2009-10-22. (<http://www.nytimes.com/2009/10/23/technology/23net.html> 2009-12-18.)

Rickardsson, André, *"Antipiratbyrån kan ha begått dataintrång"*, Svenska Dagbladet 2009-04-05. (http://www.svd.se/opinion/brannpunkt/antipiratbyran-kan-ha-begatt-dataintrang_2701391.svd 2009-12-18.)

Rosén, Hans, *Bakgrund: Striden om Telekompaketet*, Dagens Nyheter 2009-04-27. (<http://www.dn.se/fordjupning/europa2009/bakgrund-striden-om-telekompaketet-1.853549> 2009-12-18.)

- Rosén, Hans, *EU-nej till att stänga av fildelare*, Dagens Nyheter 2009-04-21. (<http://www.dn.se/kultur-noje/eu-nej-till-att-stanga-av-fildelare-1.849460> 2009-12-18.)
- Rosén, Hans, *Internetanvändarens guide till EU:s telekompaket*, Dagens Nyheter 2009-03-31. (<http://www.dn.se/fordjupning/europa2009/internetanvandarens-guide-till-eus-telekompaket-1.833955> 2009-12-18.)
- Rosén, Hans, *Kompromiss om telekompaketet klar i natt*, Dagens Nyheter 2009-11-05. (<http://www.dn.se/fordjupning/europa2009/kompromiss-om-telekompaketet-klar-i-natt-1.988539> 2009-12-18.)
- Rosén, Hans, *Liberalt sidbyte stoppade Telekompaketet*, Dagens Nyheter 2009-05-06. (<http://www.dn.se/kultur-noje/liberalt-sidbyte-stoppade-telekompaketet-1.859662> 2009-12-18.)
- Stenberg, Ewa, *Nya IT-lagar kostar hushållen miljarder*, Dagens Nyheter 2008-11-30. (<http://www.dn.se/nyheter/sverige/nya-it-lagar-kostar-hushallen-miljarder-1.470325> 2009-12-18.)
- Stiernstedt, Jenny, *”En krigsförklaring mot internet”*, Dagens Nyheter 2009-04-16. (<http://www.dn.se/kultur-noje/ipred-acta-telekompaketet-the-pirate-bay-1.845128> 2009-12-18.)
- Stiernstedt, Jenny, *EU röstar om friheten på nätet*, Dagens Nyheter 2009-03-31. (<http://www.dn.se/fordjupning/europa2009/eu-rostar-om-friheten-pa-natet-1.833938> 2009-12-18.)
- Stiernstedt, Jenny, *Hård slutstrid om internets framtid*, Dagens Nyheter 2009-04-15. (<http://www.dn.se/kultur-noje/forhandlingar-i-bryssel-om-eus-telekompaket-1.844537> 2009-12-18.)
- Stiernstedt, Jenny, *Internettrafiken minskade*, Dagens Nyheter 2009-04-02. (<http://www.dn.se/kultur-noje/internettrafiken-minskade-1.836372> 2009-12-18.)
- Ståhl, Henrik, *Telekompaketet slutförhandlat*, Svenska Dagbladet 2009-11-05. (http://www.svd.se/nyheter/inrikes/telekompaketet-slutforhandlat_3754299.svd 2009-12-18.)
- Svahn, Clas, *Telekompaketet: Strid om rättssäkerhet in i det sista*, Dagens Nyheter 2009-05-05. (<http://www.dn.se/fordjupning/europa2009/telekompaketet-strid-om-rattssakerhet-in-i-det-sista-1.858591> 2009-12-18.)

- Svantesson, Erika, "Vi har inget att välja på", Dagens Nyheter 2009-05-15. (<http://www.dn.se/nyheter/politik/vi-har-inget-att-valja-pa-1.867315> 2009-12-18.)
- Svantesson, Erika, *Tele 2 går runt Ipredlagen*, Dagens Nyheter 2009-04-27. (<http://www.dn.se/kultur-noje/film-tv/tele-2-gar-runt-ipredlagen-1.853592> 2009-12-18.)
- SVD.SE, *Lagen om datalagring upprör*, Svenska Dagbladet 2008-12-13. (http://www.svd.se/nyheter/inrikes/lagen-om-datalagring-uppror_2197461.svd 2009-12-18.)
- TT, *Bredbandsoperatör döljer fildelande*, Sydsvenskan 2009-05-14. (<http://sydsvenskan.se/kultur-och-nojen/article431819/Bredbandsoperator-doljer-fildelande.html> 2009-12-18.)
- TT-Reuters, *Fortsatt strid om fransk fildelarlag*, Dagens Nyheter 2009-09-15. (<http://www.dn.se/nyheter/varlden/fortsatt-strid-om-fransk-fildelarlag-1.953438> 2009-12-18.)
- TT-AFP, *Fransk lag mot nätpirater godkänd*, Svenska Dagbladet 2009-09-22. (http://www.svd.se/naringsliv/nyheter/fransk-lag-mot-natpirater-godkand_3558525.svd 2009-12-18.)
- TT, *Full fart på fildelningen igen*, Dagens Nyheter 2009-06-18. (<http://www.dn.se/kultur-noje/nyheter/full-fart-pa-fildelningen-igen-1.894183> 2009-12-18.)
- TT, *Ipredlagen utvärderas*, Dagens Nyheter 2009-07-23. (<http://www.dn.se/nyheter/sverige/ipredlagen-utvarderas-1.917051> 2009-12-18.)
- TT-AFP, *Nej till fildelningslag i Frankrike*, Dagens Nyheter 2009-06-10. (<http://www.dn.se/kultur-noje/nyheter/nej-till-fildelningslag-i-frankrike-1.888864> 2009-12-18.)
- TT, *Regeringen skjuter sönder Ipred*, Sydsvenskan 2009-05-19. (<http://sydsvenskan.se/sverige/article432787/Regeringen-skjuter-sonder-Ipred.html> 2009-12-18.)
- TT, *Regeringen skjuter på datalagring*, Svenska Dagbladet 2009-10-21. (http://www.svd.se/nyheter/inrikes/regeringen-skjuter-pa-datalagring_3686789.svd 2009-12-18.)

Övrigt, för referens

Bahnhof remissyttrande SOU 2007:76. Finns på
http://www.frendo.se/dokument/td_bahnhof.pdf (2009-12-18).

Blackout Europe – Defending the Open Internet. <http://blackouteurope.eu/>
(2009-12-18).

iNTeGriTY – integritetsmärkt bredband. <http://integrity.st/> (2009-12-18).

IPtegrity.com. <http://www.iptegrity.com/> (2009-12-18).

Hjemmet Mortensens produktbeskrivning av Datormagazin.
<http://www.hjemmetmortensen.se/produkter/datormagazin/>
(2009-12-18).

La Quadrature du Net. <http://www.laquadrature.net/> (2009-12-18).

TeliaSoneras remissvar över Trafikuppgiftsutredningens betänkande
Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76).
Finns på http://www.frendo.se/dokument/td_teliasonera.pdf
(2009-12-18).

Tidningsstatistik AB:s information om tidskriften Datormagazin.
<http://www.ts.se/Mediefakta/Index.aspx?mc=004306>
(2009-12-18).

We Rebuild. <http://werebuild.eu/> (2009-12-18).

Rättsfallsförteckning

EG-domstolens dom C-275/06.

EG-domstolens dom C-301/06.

EG-domstolens dom C-341/07.

Romania Constitutional Court Decision no.1258 from 8 October 2009.

Regarding the unconstitutionality exception of the provisions of Law no.298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of law 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area. Finns på <http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html> och som pdf på http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (2009-12-18).

Svea hovrätts beslut ÖÄ 6091-09.